(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2001 年10 月18 日 (18.10.2001)

PCT

(10) 国際公開番号
WO 01/78301 A1

(51) 国際特許分類[7]: H04L 9/00, G11B 20/10, 20/12

(21) 国際出願番号: PCT/JP01/03004

(22) 国際出願日: 2001 年4 月6 日 (06.04.2001)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:

特願2000-105328	2000 年4 月6 日 (06.04.2000)	JP
特願2000-106039	2000 年4 月7 日 (07.04.2000)	JP
特願2000-170604	2000 年6 月7 日 (07.06.2000)	JP
特願2000-391976	2000 年12 月25 日 (25.12.2000)	JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).

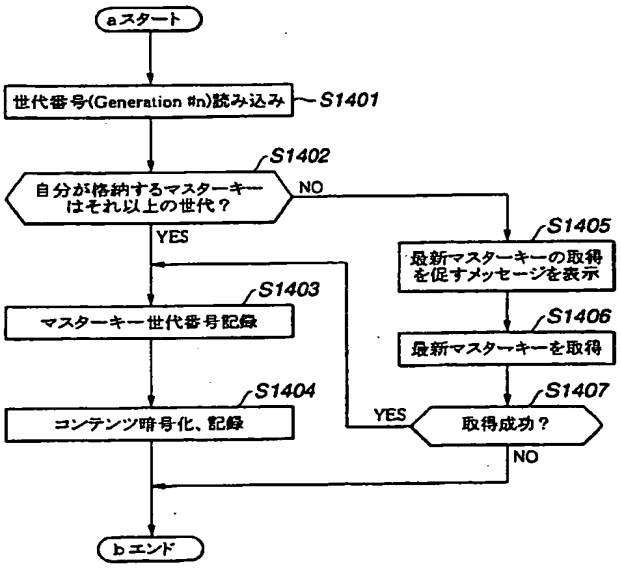
(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 浅野智之 (ASANO, Tomoyuki) [JP/JP]. 大澤義知 (OSAWA, Yoshitomo) [JP/JP]. 石黒隆二 (ISHIGURO, Ryuji) [JP/JP]. 光澤 敦 (MITSUZAWA, Atsushi) [JP/JP]. 大石丈於 (OISHI, Fateo) [JP/JP]. 瀧 隆太 (TAKI, Ryuta) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 小池 晃, 外(KOIKE, Akira et al.); 〒105-0001 東京都港区虎ノ門二丁目6番4号 第11森ビル Tokyo (JP).

[続葉有]

(54) Title: INFORMATION RECORDING/REPRODUCING APPARATUS AND METHOD

(54) 発明の名称: 情報記録/再生装置及び方法



a...START
S1401...READ GENERATION NUMBER (Generation #n)
S1402...GENERATION NUMBER OF MASTER KEY THAT THE APPARATUS HAS IS THE SAME AS OR LAGER THAN THAT READ AT S1401
S1403...RECORD GENERATION NUMBER OF MASTER KEY
S1404...CIPHER CONTENT AND RECORD CIPHERED CONTENT
S1405...DISPLAY MESSAGE TO PROMPT THE USER TO ACQUIRE LATEST MASTER KEY
S1406...ACQUIRE LATEST MASTER KEY
S1407...SUCCESSFUL ACQUISITION?
b...END

(57) Abstract: If the generation of a master key that a reproducing apparatus has is older than that used when data is recorded and consequently the data cannot be reproduced, or if the generation of a master key that a recording apparatus has is older than that required when data is to be recorded on a record medium and consequently the data cannot be recorded, the user is prompted to update the master key, and the user acquires a required master key to perform reproducing or recording. the updated master key is delivered in the form handled only by a specific device through a transmission medium such as a record medium, a network, an IC card, or a telephone line by using, e.g., a tree-structured key delivery system.

[続葉有]

WO 01/78301 A1

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

再生機器が持つマスターキーの世代がデータの記録時に用いられたものよりも古く再生ができない場合、及び記録機器が持つマスターキーの世代が記録媒体の記録に必要なものよりも古く記録ができない場合に、ユーザに対してマスターキーの更新を促し、必要なマスターキーを入手して再生処理又は記録処理を可能とする。更新マスターキーは、記録媒体、ネットワーク、ＩＣカード、電話回線などの伝送媒体を用い、例えばツリー型キー配信構成を用いて、特定のデバイスにおいてのみ処理可能な形態で配信する。

明細書

情報記録／再生装置及び方法

技術分野

本発明は、情報記録装置、情報再生装置、情報記録方法、情報再生方法、キー更新端末装置、世代管理キー更新方法、及び情報記録媒体、並びにプログラム提供媒体に関し、特に、データ記録再生可能な記録媒体に対するデータ書き込み、データ再生処理における違法コピーを防止することを可能とした情報記録装置、情報再生装置、情報記録方法、情報再生方法、キー更新端末装置、世代管理キー更新方法、及び情報記録媒体、並びにプログラム提供媒体に関する。

背景技術

ディジタル信号処理技術の進歩、発展に伴い、近年においては、情報を、ディジタル的に記録する記録装置や記録媒体が普及しつつある。このようなディジタル記録装置及び記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことができる。このようにディジタルデータは画質や音質を維持したまま何度もコピーを繰り返し実行することができるため、コピーが違法に行われた記録媒体が市場に流通することになると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害されることになる。昨今では、このようなディジタルデータの不正なコピーを防ぐため、ディジタル記録装置及び記録媒体に違法なコピーを防止するための様々な仕組み（システム）が導入されている。

例えば、ＭＤ（ミニディスク）（ＭＤは商標）装置において、違法なコピーを防止する方法として、ＳＣＭＳ（Serial Copy Management System）が採用されている。ＳＣＭＳは、データ再生側において、オーディオデータとともにＳＣＭＳ

信号をディジタルインタフェース（ＤＩＦ）から出力し、データ記録側において、再生側からのＳＣＭＳ信号に基づいて、再生側からのオーディオデータの記録を制御することにより違法なコピーを防止するシステムである。

具体的にはＳＣＭＳ信号は、オーディオデータが、何度でもコピーが許容されるコピーフリー（copy free）のデータであるか、１度だけコピーが許されている（copy once allowed）データであるか、又はコピーが禁止されている（copy prohibited）データであるかを表す信号である。データ記録側において、ＤＩＦからオーディオデータを受信すると、そのオーディオデータとともに送信されるＳＣＭＳ信号を検出する。そして、ＳＣＭＳ信号が、コピーフリー（copy free）となっている場合には、オーディオデータをＳＣＭＳ信号とともにミニディスクに記録する。また、ＳＣＭＳ信号が、コピーを１度のみ許可（copy once allowed）となっている場合には、ＳＣＭＳ信号をコピー禁止（copy prohibited）に変更して、オーディオデータとともに、ミニディスクに記録する。さらに、ＳＣＭＳ信号が、コピー禁止（copy prohibited）となっている場合には、オーディオデータの記録を行わない。このようなＳＣＭＳを使用した制御を行うことで、ミニディスク装置では、ＳＣＭＳによって、著作権を有するオーディオデータが、違法にコピーされるのを防止するようになっている。

しかしながら、ＳＣＭＳは上述のようにＳＣＭＳ信号に基づいて再生側からのオーディオデータの記録を制御する構成をデータを記録する機器自体が有していることが前提であるため、ＳＣＭＳの制御を実行する構成を持たないミニディスク装置が製造された場合には、対処するのが困難となる。そこで、例えば、ＤＶＤプレーヤでは、コンテンツ・スクランブルシステムを採用することにより、著作権を有するデータの違法コピーを防止する構成となっている。

コンテンツ・スクランブルシステムでは、ＤＶＤ－ＲＯＭ（Read Only Memory）に、ビデオデータやオーディオデータ等が暗号化されて記録されており、その暗号化されたデータを復号するのに用いるキー（復号鍵）が、ライセンスを受けたＤＶＤプレーヤに与えられる。ライセンスは、不正コピーを行わない等の所定の動作規定に従うように設計されたＤＶＤプレーヤに対して与えられる。したがって、ライセンスを受けたＤＶＤプレーヤでは、与えられたキーを利用して、Ｄ

ＶＤ－ＲＯＭに記録された暗号化データを復号することにより、ＤＶＤ－ＲＯＭから画像や音声を再生することができる。

一方、ライセンスを受けていないＤＶＤプレーヤは、暗号化されたデータを復号するためのキーを有していないため、ＤＶＤ－ＲＯＭに記録された暗号化データの復号を行うことができない。このように、コンテンツ・スクランブルシステム構成では、ライセンス時に要求される条件を満たしていないＤＶＤプレーヤは、ディジタルデータを記録したＤＶＤ－ＲＯＭの再生を行えないことになり、不正コピーが防止されるようになっている。

しかしながら、ＤＶＤ－ＲＯＭで採用されているコンテンツ・スクランブルシステムは、ユーザによるデータの書き込みが不可能な記録媒体（以下、適宜、ＲＯＭメディアという）を対象としており、ユーザによるデータの書き込みが可能な記録媒体（以下、適宜、ＲＡＭメディアという）への適用については考慮されていない。

すなわち、ＲＯＭメディアに記録されたデータが暗号化されていても、その暗号化されたデータを、そのまま全部、ＲＡＭメディアにコピーした場合には、ライセンスを受けた正当な装置で再生可能な、いわゆる海賊版を作成することができてしまう。

そこで、本出願人は、先の特許出願、特開平１１－２２４４６１号公報（特願平１０－２５３１０号）において、個々の記録媒体を識別するための情報（以下、媒体識別情報と記述する）を、他のデータとともに記録媒体に記録し、この媒体識別情報のライセンスを受けた装置であることを条件として、その条件が満たされた場合にのみ記録媒体の媒体識別情報へのアクセスが可能となる構成を提案した。

この方法では、記録媒体上のデータは、媒体識別情報とライセンスを受けることにより得られる秘密キー（マスターキー）により暗号化され、ライセンスを受けていない装置が、この暗号化されたデータを読み出したとしても、意味のあるデータを得ることができないようになっている。なお、装置はライセンスを受ける際、不正な複製（違法コピー）ができないように、その動作が規定される。

ライセンスを受けていない装置は、媒体識別情報にアクセスできず、また、媒

ターキーを用いてデータを暗号化して記録するようにしている。このため、古い記録媒体であっても、正当な機器によって最新に近いマスターキーを用いてデータが暗号化され記録されるため、最新のマスターキーを得られない、秘密が暴かれた機器によりこのデータが読まれるのを防ぐことができる。

上述の世代管理マスターキーを用いる構成においては、記録機器は自身が持つ最新の世代のマスターキーを用いてデータを暗号化して記録する。その記録媒体が別の再生機器によって再生されるためには、再生機器が記録時に使用された世代のマスターキーを知っている必要があるが、最新世代のマスターキーは最新世代の記録媒体にアクセスしなければ得られないため、これができていず、正当な再生機器であっても記録されたデータを再生できないことが起こりうる。

また、記録時には、記録機器が記録媒体が許可する世代以上に新しいマスターキーを持つことが必要であるが、ある機器グループの秘密が暴かれたために、記録媒体のマスターキーテーブルからこのグループ用の暗号化マスターキーが取り除かれている可能性があり、この記録機器が正当なものであってもこの記録媒体にデータを記録できないことが起こりうる。

発明の開示

本発明はこのような状況に鑑みてなされたものであり、不正にデータが複製されることを防止する特徴を保ったまま、インタオペラビリティをより広く確保することを可能とする情報記録装置、情報再生装置、情報記録方法、情報再生方法、キー更新端末装置、世代管理キー更新方法、及び情報記録媒体、並びにプログラム提供媒体を提供することを目的とする。

本発明の第1の側面は、記録媒体に情報を記録する情報記録装置において、世代毎に更新され、異なるキーとして設定される世代管理暗号化キーに基づく暗号処理によって前記記録媒体に対する格納情報の暗号処理を実行する暗号処理手段と、前記情報記録装置の記憶手段に格納された装置格納世代管理暗号化キーの世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報とを比較し、前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報

体識別情報は個々の媒体毎に個別の値となっているため、ライセンスを受けていない装置が、記録媒体に記録されている、暗号化されたデータの全てを新たな記録媒体に複製したとしても、そのようにして作成された記録媒体に記録されたデータは、ライセンスを受けていない装置は勿論、ライセンスを受けた装置においても、正しく復号することができないから、実質的に、違法コピーが防止されることになる。

しかし、先の提案におけるライセンスにより得られる秘密キー（マスターキー）は、全機器おいて共通である必要があった。これは、所定の機器で記された記録媒体を、他の機器においても再生可能とするインタオペラビリティを確保するための必要な条件であるからである。

しかし、この共通マスターキーを格納する構成であるがために、１つの機器が攻撃者より攻撃を受け、その機器が保持していた秘密キーが暴かれてしまった場合、全ての機器の秘密キーが暴かれてしまったのと同じ結果を招くことになり、秘密キーが暴かれる前に記録されたデータは勿論、秘密キーが暴かれた後に記録されたデータ、その暴かれた秘密キーを用いて、解読されてしまうという課題があった。

そこで、本件出願人は先に提案した特願平１１－２９４９２８号において、上記マスターキーを世代管理する方法を提案した。すなわち、全システムで共通なマスターキーを第１世代から使用していき、機器グループ毎に固有の秘密キーを用いることにより記録媒体からその記録媒体が生産された時点の最新のマスターキーを各機器が入手できるようにした構成である。すなわち、格納キーの秘密が暴かれたグループについては、それ以降に生産される記録媒体においては次の世代のマスターキーを与えないようにしている。このようにすることで、正当な（秘密が暴かれていない）機器はより新しい世代のマスターキーを得られるが、秘密が暴かれた機器はある世代のマスターキーを最後にそれより新しいものは得られないように構成したものである。

記録機器がデータを記録媒体に記録する際には、記録媒体に格納されたマスターキーと同じ世代かより新しい世代のマスターキーを使用してのみ記録することができ、その条件に合うマスターキーを持つ記録機器は、自分が持つ最新のマス

よりも新しいものである場合に、警告出力を実行するユーザインタフェースと、を有することを特徴とする情報記録装置にある。

さらに、本発明の情報記録装置の一実施態様において、前記装置格納世代管理暗号化キーは、複数の情報記録装置に共通に格納されたマスターキーであることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、前記プレ世代情報の示す世代と同世代以降の世代管理暗号化キーに更新処理を実行する更新手段を含むことを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記装置格納世代管理暗号化キーの世代情報よりも古い世代情報の世代管理暗号化キーを、前記装置格納世代管理暗号化キーに基づいて生成するキー生成手段を有する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、前記プレ世代情報の示す世代と同世代以降の世代管理暗号化キーに更新処理を実行する更新手段を含み、前記更新手段は、暗号化処理の施された更新用世代管理暗号化キーについての復号処理を、前記情報記録装置に格納されたデバイスキーに基づいて実行し、更新された世代管理暗号化キーを生成する構成を有することを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記暗号化処理の施された更新用世代管理暗号化キーと、復号用のデバイスキー識別子とを対応付けたキーテーブルを取得して、該キーテーブル中のデバイスキー識別子に基づいて識別されるデバイスキーにより、前記暗号化処理の施された更新用世代管理暗号化キーについての復号処理を実行する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記デバイスキーは、情報記録装置をカテゴリ区分し、共通のカテゴリに属する情報記録装置に共通のキーとした構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記デバイスキーは、情報記録装置に付与されたシリアルナンバの区分に基づいて共通のキーとした構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記情報記録装置は、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、前記世代管理暗号化キーは、前記ノードキー又はリーフキーの少なくともいずれかを用いて更新可能なキーとして構成されていることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記世代管理暗号化キーは、複数の情報記録装置において共通なマスターキーであることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報記録装置に配布する構成であり、前記情報記録装置における前記暗号処理手段は、前記更新ノードキーで暗号化処理した前記世代管理暗号化キーの更新データを受領し、キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記世代管理暗号化キーの更新データを取得する構成を有することを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記キー更新ブロック（ＫＲＢ）は、記録媒体に格納され、前記暗号処理手段は、前記記録媒体から読み出されたキー更新ブロック（ＫＲＢ）についての暗号処理を実行する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記世代管理暗号化キーは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理部は、前記記録媒体に対する暗号化データ格納時に、使用した前記世代管理暗号化キーの世代番号を記録時世代番号として前記記録媒体に格納する構成を有することを特徴とする。

さらに、本発明の第２の側面は、記録媒体に情報を記録する情報記録装置にお

いて、世代毎に更新され、異なるキーとして設定される世代管理暗号化キーに基づく暗号処理によって前記記録媒体に対する格納情報の暗号処理を実行する暗号処理手段と、前記情報記録装置の記憶手段に格納された装置格納世代管理暗号化キーの世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報とを比較し、前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、前記プレ世代情報の示す世代又は該世代以降の世代管理暗号化キーの取得を実行するキー取得手段と、を有することを特徴とする情報記録装置にある。

さらに、本発明の情報記録装置の一実施態様において、前記キー取得手段は、ネットワークを介するデータ受信の実行可能な通信インタフェースを含むことを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記キー取得手段は、電話回線を介するデータ受信の実行可能な通信モデムを含むことを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記キー取得手段は、ＩＣカードを介するデータ受信の実行可能なＩ／Ｃカードインタフェースを含むことを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記キー取得手段によるキー取得実行の際に、キー提供手段との相互認証処理を実行する構成を有し、前記キー取得手段は、前記相互認証処理の成立を条件として前記世代管理暗号化キーの取得を実行する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記装置格納世代管理暗号化キーは、複数の情報記録装置に共通に格納されたマスターキーであることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、前記プレ世代情報の示す世代と同世代以降の世代管理暗号化キーに更新処理を実行する更新手段を含むことを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記装置格納世代管理暗号化キーの世代情報よりも古い世代情報の世代管理暗号

化キーを、前記装置格納世代管理暗号化キーに基づいて生成するキー生成手段を有する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、前記プレ世代情報の示す世代と同世代以降の世代管理暗号化キーに更新処理を実行する更新手段を含み、前記更新手段は、暗号化処理の施された更新用世代管理暗号化キーについての復号処理を、前記情報記録装置に格納されたデバイスキーに基づいて実行し、更新された世代管理暗号化キーを生成する構成を有することを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記暗号処理手段は、前記暗号化処理の施された更新用世代管理暗号化キーと、復号用のデバイスキー識別子とを対応付けたキーテーブルを取得して、該キーテーブル中のデバイスキー識別子に基づいて識別されるデバイスキーにより、前記暗号化処理の施された更新用世代管理暗号化キーについての復号処理を実行する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記デバイスキーは、情報記録装置をカテゴリ区分し、共通のカテゴリに属する情報記録装置に共通のキーとした構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記デバイスキーは、情報記録装置に付与されたシリアルナンバの区分に基づいて共通のキーとした構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記情報記録装置は、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、前記世代管理暗号化キーは、前記ノードキー又はリーフキーの少なくともいずれかを用いて更新可能なキーとして構成されていることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記世代管理暗号化キーは、複数の情報記録装置において共通なマスターキーであることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記ノードキーは更新

可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報記録装置に配布する構成であり、前記情報記録装置における前記暗号処理手段は、前記更新ノードキーで暗号化処理した前記世代管理暗号化キーの更新データを受領し、キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記世代管理暗号化キーの更新データを取得する構成を有することを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記キー更新ブロック（ＫＲＢ）は、記録媒体に格納され、前記暗号処理手段は、前記記録媒体から読み出されたキー更新ブロック（ＫＲＢ）についての暗号処理を実行する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記世代管理暗号化キーは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理部は、前記記録媒体に対する暗号化データ格納時に、使用した前記世代管理暗号化キーの世代番号を記録時世代番号として前記記録媒体に格納する構成を有することを特徴とする。

さらに、本発明の第３の側面は、記録媒体に情報を記録する情報記録装置において、世代毎に更新され、異なるキーとして設定される世代管理暗号化キーに基づく暗号処理によって前記記録媒体に対する格納情報の暗号処理を実行する暗号処理手段と、前記情報記録装置の記憶手段に格納された装置格納世代管理暗号化キーの世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報とを比較し、前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、前記プレ世代情報の示す世代又は該世代以降の世代管理暗号化キーを取得するためのキー更新端末を接続するキー更新端末接続インタフェースと、を有することを特徴とする情報記録装置にある。

さらに、本発明の情報記録装置の一実施態様は、前記キー更新端末からの前記世代管理暗号化キー取得実行の際に、前記キー更新端末との相互認証処理を実行する構成を有し、前記情報記録装置は、前記相互認証処理の成立を条件として前

記世代管理暗号化キーの取得を実行する構成である。

さらに、本発明の情報記録装置の一実施態様において、前記情報記録装置は、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、前記世代管理暗号化キーは、前記ノードキー又はリーフキーの少なくともいずれかを用いて更新可能なキーとして構成されていることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記世代管理暗号化キーは、複数の情報記録装置において共通なマスターキーであることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報記録装置に配布する構成であり、前記情報記録装置における前記暗号処理手段は、前記更新ノードキーで暗号化処理した前記世代管理暗号化キーの更新データを受領し、キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記世代管理暗号化キーの更新データを取得する構成を有することを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記キー更新ブロック（ＫＲＢ）は、記録媒体に格納され、前記暗号処理手段は、前記記録媒体から読み出されたキー更新ブロック（ＫＲＢ）についての暗号処理を実行する構成であることを特徴とする。

さらに、本発明の情報記録装置の一実施態様において、前記世代管理暗号化キーは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理部は、前記記録媒体に対する暗号化データ格納時に、使用した前記世代管理暗号化キーの世代番号を記録時世代番号として前記記録媒体に格納する構成を有することを特徴とする。

さらに、本発明の第４の側面は、記録媒体から情報を再生する情報再生装置において、世代毎に更新され、異なるキーとして設定される世代管理復号キーに基づく復号処理によって前記記録媒体から読み取られる情報の復号処理を実行する

暗号処理手段と、前記情報再生装置の記憶手段に格納された装置格納世代管理復号キーの世代情報と、前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報とを比較し、前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、警告出力を実行するユーザインタフェースと、を有することを特徴とする情報再生装置にある。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報との比較処理において前記プレ世代情報が前記記録時世代情報よりも新しいものである場合に復号処理を実行しない構成としたことを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記装置格納世代管理復号キーは、複数の情報再生装置に共通に格納されたマスターキーであることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、前記記録時世代情報の示す世代と同世代以降の世代管理復号キーに更新処理を実行する更新手段を含むことを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記装置格納世代管理復号キーの世代情報よりも古い世代情報の世代管理復号キーを、前記装置格納世代管理復号キーに基づいて生成するキー生成手段を有する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、前記記録時世代情報の示す世代と同世代以降の世代管理復号キーに更新処理を実行する更新手段を含み、前記更新手段は、暗号化処理の施された更新用世代管理復号キーについての復号処理を、前記情報再生装置に格納されたデバイスキーに基づいて実行し、更新された世代管理復号キーを生成する構成を有することを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、

前記暗号化処理の施された更新用世代管理復号キーと、復号用のデバイスキー識別子とを対応付けたキーテーブルを取得して、該キーテーブル中のデバイスキー識別子に基づいて識別されるデバイスキーにより、前記暗号化処理の施された更新用世代管理復号キーについての復号処理を実行する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記デバイスキーは、情報再生装置をカテゴリ区分し、共通のカテゴリに属する情報再生装置に共通のキーとした構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記デバイスキーは、情報再生装置に付与されたシリアルナンバの区分に基づいて共通のキーとした構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記情報再生装置は、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、前記世代管理復号キーは、前記ノードキー又はリーフキーの少なくともいずれかを用いて更新可能なキーとして構成されていることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記世代管理復号キーは、複数の情報再生装置において共通なマスターキーであることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報再生装置に配布する構成であり、前記情報再生装置における前記暗号処理手段は、前記更新ノードキーで暗号化処理した前記世代管理復号キーの更新データを受領し、キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記世代管理復号キーの更新データを取得する構成を有することを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記キー更新ブロック（ＫＲＢ）は、記録媒体に格納され、前記暗号処理手段は、前記記録媒体から読

み出されたキー更新ブロック（ＫＲＢ）についての暗号処理を実行する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記世代管理復号キーは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理部は、前記記録媒体からの暗号化データの復号時に、該暗号化データの暗号処理時に使用した世代管理暗号化キーの世代番号を前記記録媒体から読み取り、該読み取られた世代番号に対応する世代管理復号キーを使用して復号を実行する構成であることを特徴とする。

さらに、本発明の第５の側面は、記録媒体から情報を再生する情報再生装置において、世代毎に更新され、異なるキーとして設定される世代管理復号キーに基づく復号処理によって前記記録媒体から読み取られる情報の復号処理を実行する暗号処理手段と、前記情報再生装置の記憶手段に格納された装置格納世代管理復号キーの世代情報と、前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報とを比較し、前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、前記記録時世代情報の示す世代又は該世代以降の世代管理復号キーの取得を実行するキー取得手段と、を有することを特徴とする情報再生装置にある。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報との比較処理において前記プレ世代情報が前記記録時世代情報よりも新しいものである場合に復号処理を実行しない構成としたことを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記キー取得手段は、ネットワークを介するデータ受信の実行可能な通信インタフェースを含むことを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記キー取得手段は、電話回線を介するデータ受信の実行可能な通信モデムを含むことを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記キー取得手段は、ＩＣカードを介するデータ受信の実行可能なＩ／Ｃカードインタフェースを含む

ことを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記キー取得手段によるキー取得実行の際に、キー提供手段との相互認証処理を実行する構成を有し、前記キー取得手段は、前記相互認証処理の成立を条件として前記世代管理復号キーの取得を実行する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記装置格納世代管理復号キーは、複数の情報再生装置に共通に格納されたマスターキーであることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、前記記録時世代情報の示す世代と同世代以降の世代管理復号キーに更新処理を実行する更新手段を含むことを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記装置格納世代管理復号キーの世代情報よりも古い世代情報の世代管理復号キーを、前記装置格納世代管理復号キーに基づいて生成するキー生成手段を有する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、前記記録時世代情報の示す世代と同世代以降の世代管理復号キーに更新処理を実行する更新手段を含み、前記更新手段は、暗号化処理の施された更新用世代管理復号キーについての復号処理を、前記情報再生装置に格納されたデバイスキーに基づいて実行し、更新された世代管理復号キーを生成する構成を有することを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記暗号処理手段は、前記暗号化処理の施された更新用世代管理復号キーと、暗号復号用のデバイスキー識別子とを対応付けたキーテーブルを取得して、該キーテーブル中のデバイスキー識別子に基づいて識別されるデバイスキーにより、前記暗号化処理の施された更新用世代管理復号キーについての復号処理を実行する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記デバイスキーは、情報再生装置をカテゴリ区分し、共通のカテゴリに属する情報再生装置に共通のキーとした構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記デバイスキーは、情報再生装置に付与されたシリアルナンバの区分に基づいて共通のキーとした構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記情報再生装置は、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、前記世代管理復号キーは、前記ノードキー又はリーフキーの少なくともいずれかを用いて更新可能なキーとして構成されていることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記世代管理復号キーは、複数の情報再生装置において共通なマスターキーであることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報再生装置に配布する構成であり、前記情報再生装置における前記暗号処理手段は、前記更新ノードキーで暗号化処理した前記世代管理復号キーの更新データを受領し、キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記世代管理復号キーの更新データを取得する構成を有することを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記キー更新ブロック（ＫＲＢ）は、記録媒体に格納され、前記暗号処理手段は、前記記録媒体から読み出されたキー更新ブロック（ＫＲＢ）についての暗号処理を実行する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記世代管理復号キーは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理部は、前記記録媒体からの暗号化データの復号時に、該暗号化データの暗号処理時に使

用した世代管理暗号化キーの世代番号を前記記録媒体から読み取り、該読み取られた世代番号に対応する世代管理復号キーを使用して復号を実行する構成であることを特徴とする。

さらに、本発明の第６の側面は、記録媒体から情報を再生する情報再生装置において、世代毎に更新され、異なるキーとして設定される世代管理復号キーに基づく復号処理によって前記記録媒体から読み取られる情報の復号処理を実行する暗号処理手段と、前記情報再生装置の記憶手段に格納された装置格納世代管理復号キーの世代情報と、前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報とを比較し、前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、前記記録時世代情報の示す世代又は該世代以降の世代管理復号キーを取得するためのキー更新端末を接続するキー更新端末接続インタフェースと、を有することを特徴とする情報再生装置にある。

さらに、本発明の情報再生装置の一実施態様において、前記キー更新端末からの前記世代管理復号キー取得実行の際に、前記キー更新端末との相互認証処理を実行する構成を有し、前記情報再生装置は、前記相互認証処理の成立を条件として前記世代管理復号キーの取得を実行する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記情報再生装置は、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、前記世代管理復号キーは、前記ノードキー又はリーフキーの少なくともいずれかを用いて更新可能なキーとして構成されていることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記世代管理復号キーは、複数の情報再生装置において共通なマスターキーであることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報再生装置に配布する構成であり、前記情報再生装置における前記暗号処理手段は、前記更新ノードキーで

暗号化処理した前記世代管理復号キーの更新データを受領し、キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記世代管理復号キーの更新データを取得する構成を有することを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記キー更新ブロック（ＫＲＢ）は、記録媒体に格納され、前記暗号処理手段は、前記記録媒体から読み出されたキー更新ブロック（ＫＲＢ）についての暗号処理を実行する構成であることを特徴とする。

さらに、本発明の情報再生装置の一実施態様において、前記世代管理復号キーは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理部は、前記記録媒体からの暗号化データの復号時に、該暗号化データの暗号処理時に使用した世代管理暗号化キーの世代番号を前記記録媒体から読み取り、該読み取られた世代番号に対応する世代管理復号キーを使用して復号を実行する構成であることを特徴とする。

さらに、本発明の第７の側面は、記録媒体に情報を記録する情報記録方法において、世代毎に更新され、異なるキーとして設定される世代管理暗号化キーに基づく暗号処理によって前記記録媒体に対する格納情報の暗号処理を実行する暗号処理ステップを有し、さらに、情報記録装置の記憶手段に格納された装置格納世代管理暗号化キーの世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報とを比較するステップと、前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、警告出力を実行する警告出力ステップと、を有することを特徴とする情報記録方法にある。

さらに、本発明の第８の側面は、記録媒体に情報を記録する情報記録方法において、世代毎に更新され、異なるキーとして設定される世代管理暗号化キーに基づく暗号処理によって前記記録媒体に対する格納情報の暗号処理を実行する暗号処理ステップを有し、さらに、情報記録装置の記憶手段に格納された装置格納世代管理暗号化キーの世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報とを比較するステップと、前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、前記プレ世

代情報の示す世代又は該世代以降の世代管理暗号化キーの取得を実行するキー取得ステップと、を有することを特徴とする情報記録方法にある。

さらに、本発明の情報記録方法において、前記キー取得ステップは、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーの少なくともいずれかを用いて前記世代管理暗号化キーの更新処理を実行する更新ステップと、前記更新ステップにおいて更新された世代管理暗号化キーに基づいて前記記録媒体に格納するデータの暗号処理を実行する暗号処理ステップと、を含むことを特徴とする。

さらに、本発明の情報記録方法において、前記世代管理暗号化キーは、複数の情報記録装置において共通なマスターキーであることを特徴とする。

さらに、本発明の情報記録方法において、前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報記録装置に配布する構成であり、前記更新ステップは、前記キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得する更新ノードキー取得ステップと、取得した更新ノードキーに基づいて前記世代管理暗号化キーの更新データを算出する更新データ取得ステップと、を含むことを特徴とする。

さらに、本発明の情報記録方法において、前記世代管理暗号化キーは、更新情報としての世代番号が対応付けられた構成であり、前記暗号処理ステップは、さらに、前記記録媒体に対する暗号化データ格納時に、使用した前記世代管理暗号化キーの世代番号を記録時世代番号として前記記録媒体に格納するステップを含むことを特徴とする。

さらに、本発明の第９の側面は、記録媒体から情報を再生する情報再生方法において、世代毎に更新され、異なるキーとして設定される世代管理復号キーに基づく復号処理によって前記記録媒体の格納情報の復号処理を実行する復号処理ステップを有し、さらに、情報再生装置の記憶手段に格納された装置格納世代管理復号キーの世代情報と、前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報とを比較するステップと、前記記録時世代情報が、前記

装置格納世代管理復号キーの世代情報よりも新しいものである場合に、警告出力を実行する警告出力ステップと、を有することを特徴とする情報再生方法にある。

さらに、本発明の第１０の側面は、記録媒体から情報を再生する情報再生方法において、世代毎に更新され、異なるキーとして設定される世代管理復号キーに基づく復号処理によって前記記録媒体の格納情報の復号処理を実行する復号処理ステップを有し、さらに、情報記録再生装置の記憶手段に格納された装置格納世代管理復号キーの世代情報と、前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報とを比較するステップと、前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、前記記録時世代情報の示す世代又は該世代以降の世代管理復号キーの取得を実行するキー取得ステップと、を有することを特徴とする情報再生方法にある。

さらに、本発明の情報再生方法において、前記キー取得ステップは、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーの少なくともいずれかを用いて記録媒体に格納された暗号データの復号処理を実行する世代管理復号キーの更新処理を実行する更新ステップと、前記更新ステップにおいて更新された世代管理復号キーに基づいて前記記録媒体に格納された暗号データの復号処理を実行する復号処理ステップと、を含むことを特徴とする。

さらに、本発明の情報再生方法において、前記世代管理復号キーは、複数の情報再生装置において共通なマスターキーであることを特徴とする。

さらに、本発明の情報再生方法において、前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報再生装置に配布する構成であり、前記更新ステップは、前記キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得する更新ノードキー取得ステップと、取得した更新ノードキーに基づいて前記世代管理復号キーの更新データを算出する更新データ取得ステップと、を含むことを特徴とする。

さらに、本発明の情報再生方法において、前記世代管理復号キーは、更新情報

としての世代番号が対応付けられた構成であり、前記復号処理ステップは、前記記録媒体からの暗号化データの復号時に、該暗号化データの暗号処理時に使用した世代管理暗号化キーの世代番号を前記記録媒体から読み取り、該読み取られた世代番号に対応する世代管理復号キーを使用して実行することを特徴とする。

さらに、本発明の第１１の側面は、情報の記録可能な情報記録媒体であって、該情報記録媒体に対する暗号化データの書き込みに使用可能な暗号化キー、又は該情報記録媒体の格納データの復号処理に使用可能な復号キーとして許容されるキーの世代情報としてのプレ世代情報を格納したことを特徴とする情報記録媒体にある。

さらに、本発明の情報記録媒体の一実施態様において、前記プレ世代情報は、前記情報記録媒体における書き換え不可領域に記録されていることを特徴とする。

さらに、本発明の第１２の側面は、世代毎に更新され、異なるキーとして設定される世代管理キーに基づく処理によって記録媒体に対する格納情報の暗号化処理又は記録媒体から読み取られる情報の復号処理を実行する暗号処理手段を有する情報記録又は再生装置に対する更新世代管理キーの提供を行うキー更新端末装置であり、前記情報記録又は再生装置に接続可能なインタフェースと、外部との通信を実行する通信手段と、前記インタフェースを介する前記情報記録又は再生装置からの装置固有識別子の取得処理、該装置固有識別子の前記通信手段を介する送信処理、前記通信手段を介する更新世代管理キーの受信処理、及び前記インタフェースを介する前記情報記録又は再生装置に対する更新世代管理キーの転送処理の各制御を実行する制御手段と、を有することを特徴とするキー更新端末装置にある。

さらに、本発明の第１３の側面は、世代毎に更新され、異なるキーとして設定される世代管理キーに基づく処理によって記録媒体に対する格納情報の暗号化処理又は記録媒体から読み取られる情報の復号処理を実行する暗号処理手段を有する情報記録又は再生装置に対する更新世代管理キーの提供を行うキー更新端末装置であり、前記情報記録又は再生装置に接続可能なインタフェースと、装置固有の暗号化鍵で暗号化された世代管理キーを、前記情報記録又は再生装置の装置固有識別子に対応付けたキーテーブルを格納した記憶手段と、前記インタフェース

を介する前記情報記録又は再生装置からの装置固有識別子の取得処理、該装置固有識別子に基づく前記記憶手段からの該装置固有識別子に対応する暗号化世代管理キーの取得処理、及び前記インタフェースを介する前記情報記録又は再生装置に対する更新世代管理キーの転送処理の各制御を実行する制御手段と、を有することを特徴とするキー更新端末装置にある。

さらに、本発明のキー更新端末装置の一実施態様において、前記情報記録又は再生装置との相互認証処理を実行する構成を有し、前記キー更新端末装置は、前記相互認証処理の成立を条件として前記世代管理キーの前記情報記録又は再生装置に対する提供処理を実行する構成であることを特徴とする。

さらに、本発明の第１４の側面は、世代毎に更新され、異なるキーとして設定される世代管理キーに基づく処理によって記録媒体に対する格納情報の暗号化処理又は記録媒体から読み取られる情報の復号処理を実行する暗号処理手段を有する情報記録又は再生装置に対する更新世代管理キーの提供を行う世代管理キー更新方法であり、前記情報記録又は再生装置に接続可能なインタフェースと、外部との通信を実行する通信手段とを有するキー更新端末装置を前記情報記録又は再生装置に接続するステップと、前記インタフェースを介する前記情報記録又は再生装置からの装置固有識別子の取得処理ステップと、装置固有識別子の前記通信手段を介する送信処理ステップと、前記通信手段を介する更新世代管理キーの受信処理ステップと、前記インタフェースを介する前記情報記録又は再生装置に対する更新世代管理キーの転送処理ステップと、を有することを特徴とする世代管理キー更新方法にある。

さらに、本発明の第１５の側面は、世代毎に更新され、異なるキーとして設定される世代管理キーに基づく処理によって記録媒体に対する格納情報の暗号化処理又は記録媒体から読み取られる情報の復号処理を実行する暗号処理手段を有する情報記録又は再生装置に対する更新世代管理キーの提供を行う世代管理キー更新方法であり、前記情報記録又は再生装置に接続可能なインタフェースと、装置固有の暗号化鍵で暗号化された世代管理キーを、前記情報記録又は再生装置の装置固有識別子に対応付けたキーテーブルを格納した記憶手段とを有するキー更新端末装置を前記情報記録又は再生装置に接続するステップと、前記インタフェー

スを介する前記情報記録又は再生装置からの装置固有識別子の取得処理ステップと、装置固有識別子に基づく前記記憶手段からの該装置固有識別子に対応する暗号化世代管理キーの取得処理ステップと、前記インタフェースを介する前記情報記録又は再生装置に対する更新世代管理キーの転送処理ステップと、を有することを特徴とする世代管理キー更新方法にある。

さらに、本発明の世代管理キー更新方法において、前記情報記録又は再生装置との相互認証処理を実行するステップを有し、前記相互認証処理の成立を条件として前記世代管理キーの前記情報記録又は再生装置に対する提供処理を実行することを特徴とする。

さらに、本発明の第１６の側面は、記録媒体に情報を記録する情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、情報記録装置の記憶手段に格納された装置格納世代管理暗号化キーの世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報とを比較するステップと、世代毎に更新され、異なるキーとして設定される世代管理暗号化キーに基づく暗号処理によって前記記録媒体に対する格納情報の暗号処理を実行する暗号処理ステップを有し、さらに、前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、警告出力ステップ、あるいは前記プレ世代情報の示す世代又は該世代以降の世代管理暗号化キーの取得を実行するキー取得ステップと、の少なくともいずれかを実行するステップを有することを特徴とするプログラム提供媒体にある。

さらに、本発明のプログラム提供媒体の一実施態様において、前記コンピュータ・プログラムは、さらに、複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーの少なくともいずれかを用いて記録媒体に対する格納データの暗号化処理を実行する世代管理暗号化キーの更新処理を実行する更新ステップを含むことを特徴とする。

さらに、本発明の第１７の側面は、記録媒体から情報を再生する情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供す

るプログラム提供媒体であって、前記コンピュータ・プログラムは、情報再生装置の記憶手段に格納された装置格納世代管理復号キーの世代情報と、前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報とを比較するステップと、世代毎に更新され、異なるキーとして設定される世代管理復号キーに基づく復号処理によって前記記録媒体からの格納情報の復号処理を実行する復号処理ステップを有し、さらに、前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、警告出力ステップ、あるいは前記記録時世代情報の示す世代又は該世代以降の世代管理復号キーの取得を実行するキー取得ステップと、の少なくともいずれかを実行するステップを有することを特徴とするプログラム提供媒体にある。

さらに、本発明のプログラム提供媒体の一実施態様において、前記コンピュータ・プログラムは、さらに、複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーの少なくともいずれかを用いて記録媒体に格納された暗号データの復号処理を実行する世代管理復号キーの更新処理を実行する更新ステップを含むことを特徴とする。

本発明においては、再生機器が持つマスターキーの世代がデータの記録時に用いられたものよりも古く再生ができない場合に、ユーザに対してマスターキーの更新を促し、必要なマスターキーを入手して再生処理を可能とする。マスターキーの入手は、データを記録する記録媒体以外の媒体、あるいはネットワークなどの伝送媒体を用いて行って、入手したマスターキーを用いて再生処理を行う。

また、本発明においては、記録機器が持つマスターキーの世代が記録媒体の記録に必要なものよりも古く記録ができない場合に、ユーザに対してマスターキーの更新を促し、必要なマスターキーを入手して記録処理を可能とする。マスターキーの入手は、データを記録する記録媒体以外の媒体、あるいはネットワークなどの伝送媒体を用いて行って、入手したマスターキーを用いて記録処理を行う。

なお、本発明の第１６及び第１７の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒

体は、ＣＤやＦＤ、ＭＯなどの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

図面の簡単な説明

図１は、本発明の情報記録再生装置の暗号処理部構成を示すブロック図である。

図２は、本発明の情報記録再生装置のマスターキー管理構成を示す図である。

図３は、本発明の情報記録再生装置のマスターキー更新処理フローを示す図である。

図４は、本発明の情報記録再生装置のマスターキー更新処理を示すブロック図である。

図５は、本発明の情報記録再生装置の情報再生処理フローを示す図である。

図６は、本発明の情報記録再生装置（例１）の構成を示すブロック図である。

図７は、本発明の情報記録再生装置において厳格なマスターキー世代管理を可能とした暗号処理部構成を示すブロック図である。

図８は、厳格なマスターキー世代管理を可能とした情報記録再生装置におけるマスターキー管理構成を示す図である。

図９は、厳格なマスターキー世代管理を可能とした情報記録再生装置におけるコンテンツ記録処理フローを示す図である。

図１０は、厳格なマスターキー世代管理を可能とした情報記録再生装置におけ

るマスターキー更新処理フローを示す図である。

図１１は、マスターキー世代管理を可能とした情報記録再生装置におけるマスターキー世代情報格納構成を示す図である。

図１２は、厳格なマスターキー世代管理を可能とした情報記録再生装置におけるコンテンツ再生処理フローを示す図である。

図１３は、本発明の情報記録再生装置（例２）の構成を示すブロック図である。

図１４は、厳格なマスターキー世代管理を可能とした情報記録再生装置（例２）におけるコンテンツ記録処理フローを示す図である。

図１５は、厳格なマスターキー世代管理を可能とした情報記録再生装置（例２）におけるコンテンツ再生処理フローを示す図である。

図１６は、本発明の情報記録再生装置（例３）の構成を示すブロック図である。

図１７は、厳格なマスターキー世代管理を可能とした情報記録再生装置（例３）におけるコンテンツ記録処理フローを示す図である。

図１８は、本発明の情報記録再生装置におけるキー取得処理に適用可能な認証処理（共通鍵方式）の処理シーケンスを示す図である。

図１９は、本発明の情報記録再生装置におけるキー取得処理に適用可能な認証処理（公開鍵方式）の処理シーケンスを示す図である。

図２０は、本発明の情報記録再生装置におけるキー取得処理に適用可能な認証処理に用いられる公開鍵証明書の構成を示す図である。

図２１は、本発明の情報記録再生装置におけるリボケーションリストの構成を示す図である。

図２２は、本発明の情報記録再生装置におけるレジストレーションリストの構成を示す図である。

図２３は、本発明の情報記録再生装置におけるコンテンツ再生処理フローを示す図である。

図２４は、本発明の情報記録再生装置において使用されるキー更新端末の構成を示すブロック図である。

図２５は、本発明の情報記録再生装置におけるキー更新端末を使用したキー更新処理を説明するブロック図（その１）である。

図２６は、本発明の情報記録再生装置におけるキー更新端末を使用したキー取得処理に適用可能な認証処理（共通鍵方式）の処理シーケンスを示す図である。

図２７は、本発明の情報記録再生装置におけるキー更新端末を使用したキー取得処理に適用可能な認証処理（公開鍵方式）の処理シーケンスを示す図である。

図２８は、本発明の情報記録再生装置におけるキー更新端末を使用したキー取得処理においてキー発行機関が有するキーテーブルの例を示す図である。

図２９は、本発明の情報記録再生装置におけるキー更新端末を使用したキー更新処理を説明するブロック図（その２）である。

図３０は、本発明の情報記録再生装置におけるキー更新端末を使用したキー更新処理を説明するブロック図（その３）である。

図３１は、本発明の情報記録再生装置におけるキー更新端末を使用したキー更新処理を説明するブロック図（その４）である。

図３２は、本発明の情報記録再生装置に対するマスターキー、メディアキー等の鍵の暗号化処理について説明するツリー構成図である。

図３３Ａ及び図３３Ｂは、本発明の情報記録再生装置に対するマスターキー、メディアキー等の鍵の配布に使用されるキー更新ブロック（ＫＲＢ）の例を示す図である。

図３４は、本発明の情報記録再生装置におけるマスターキーのキー更新ブロック（ＫＲＢ）を使用した配布例と復号処理例を示す図である。

図３５は、本発明の情報記録再生装置におけるマスターキーのキー更新ブロック（ＫＲＢ）を使用した復号処理フローを示す図である。

図３６は、本発明の情報記録再生装置において、外部からＫＲＢを通信手段等を介して受信し、記録媒体に格納する処理について示すブロック図である。

図３７は、本発明の情報記録再生装置において、外部からＫＲＢを通信手段等を介して受信し、記録媒体に格納する処理フローを示す図である。

図３８は、本発明の情報記録再生装置において、外部からＫＲＢを通信手段等を介して受信し、記録媒体に格納する処理を説明する図である。

図３９は、本発明のシステムにおいて利用可能な記録媒体の例を示す図である。

図４０は、本発明の情報記録再生装置において、データ処理をソフトウェアに

よって実行する場合の処理手段構成を示したブロック図である。

発明を実施するための最良の形態

［１．マスターキー世代管理の基本構成］

図１は本発明の情報再生装置１００における暗号処理部の処理機能を中心とした一実施形態の構成を示すブロック図である。情報再生装置のデバイスキー保持部１０１は、この情報再生装置１００に与えられたデバイスキーＤＫ_jを保持している。暗号文保持部１０２は、暗号化マスターキーＣ（ｊ，ｉ）（デバイスキーＤＫで暗号化されたマスターキーＭＫ_i）を保持している。このような、デバイスキーＤＫ_j、マスターキーＭＫ_i、及び暗号化マスターキーＣ（ｊ，ｉ）の関係を、Ｃ（ｊ，ｉ）＝Ｅｎｃ（ＤＫ_j，ＭＫ_i）と表す。

なお、ｉはマスターキーの世代番号を表し、ｊは、カテゴリ番号を表す。このカテゴリ番号とは、情報再生装置などのデバイスに対して割り当てられた番号であり、１台のデバイス毎、またデバイスのメーカー毎、又はデバイスのモデル毎、又はデバイスのロット毎、又は予め定められた数のデバイス、例えばデバイスに付与されたシリアルナンバの所定単位毎などに割り振られている。以下、デバイスキーＤＫ_jを、カテゴリ番号ｊを用いて区別する必要がない場合、単にデバイスキーＤＫと記述し、同様にマスターキーＭＫも、世代番号ｉを用いて区別する必要がない場合、単にマスターキーＭＫと記述する。これらに対応して、暗号化マスターキーＣ（ｊ，ｉ）も、単に暗号化マスターキーＣと記述する。

デバイスキーＤＫと暗号化マスターキーＣは、デバイスに対してキーを発行するキー発行機関から与えられ、予め記憶されている。キー発行機関は、マスターキーＭＫを保管するとともに、デバイスキーＤＫをカテゴリ番号ｊに対応付けて秘密裡に保管する。

マスターキー復号部１０３は、デバイスキー保持部１０１で保持されているデバイスキーＤＫを用いて、暗号文保持部１０２で記憶されている暗号化マスターキーＣを復号し、マスターキーＭＫを得る。すなわち、暗号文Ｘを、キーＹで復号する関数をＤＥＣ(Y,X)と表すと、マスターキー復号部１０３では、式ＭＫ_i＝

ＤＥＣ（ＤＫ_j，Ｃ(j,i)）が演算される。得られたマスターキーＭＫは、解読部１０４に供給される。

解読部１０４は、データ読み出し部１０５により、記録媒体（光ディスク）１５０などから読み出された、マスターキーＭＫに基づいて暗号化されているデータを、マスターキー復号部１０３から供給されたマスターキーＭＫを用いて解読する。すなわち、記録媒体（光ディスク）１５０には、マスターキーＭＫに基づいて暗号化されたデータが記録されており、解読部１０４は、この暗号化されたデータを、マスターキーＭＫについて解読（復号）する。解読されたデータが、例えば、画像データである場合、表示デバイスに出力され、表示される。また、データ読み出し部１０５は、後述する処理によりマスターキーＭＫを更新する場合、更新用のデータが記録された記録媒体（光ディスク）１５０から、マスターキーＭＫを、デバイスキーＤＫに基づいて暗号化した暗号化マスターキーＣを読み出し、暗号文保持部１０２に出力する。

次に、情報再生装置のマスターキーＭＫの更新について説明する。マスターキーＭＫの更新は、世代ｉのマスターキーＭＫ_iが、攻撃者などにより暴かれてしまった場合等の不定期に、あるいは所定同期で定期的に行われる。以下の説明では、マスターキー_iの更新のため、全てのデバイスのデバイスキーＤＫ_jで暗号化されたマスターキーＭＫ_i（暗号化マスターキーＣ（ｊ，ｉ））が記録された光ディスクが、キー発行機関から配布されるものとする。なお、勿論、暗号化マスターキーＣ（ｊ，ｉ）は、光ディスク以外の記録媒体や、インターネットなどネットワークを用いて配布してもよい。また、記録媒体（光ディスク）１５０は、マスターキーＭＫ_iの更新専用のものである必要はなく、ビデオデータやオーディオデータ等のコンテンツが記録されたもの、あるいはコンテンツの記録が、これから可能なものであってもよい。

図２に、記録媒体（光ディスク）１５０に記録されている暗号化マスターキーＣ（ｊ,ｉ）の例を示す。この例は、世代ｉのマスターキーＭＫ_iを世代ｉ＋１のマスターキーＭＫ_i+１に更新する場合の例である。すなわち、光ディスク１５０には、カテゴリ番号ｊと、マスターキーＭＫ_i+１を、カテゴリ番号ｊのデバイスキーＤＫ_jに基づいて暗号化した暗号化マスターキーＣ（ｊ，ｉ＋１）とが、そ

れぞれ対応付けられて記録されている。

図２に示したように、全てのカテゴリ番号ｊにおいて、マスターキーＭＫ_i+１は共通とされている。このように、各デバイスのマスターキーＭＫを共通にすることにより、ライセンスを受け、正式なデバイスキーＤＫを保持するデバイス間では、マスターキーＭＫにより暗号化されたデータを共用すること、即ち、インタオペラビリティを保つことが可能となる。また、正式なデバイスキーＤＫを保持しないデバイスは、マスターキーＭＫを復号することができないので、そのマスターキーＭＫで暗号化されたデータを復号することは不可能となる。

例えば、カテゴリ番号２のデバイスが、攻撃者から攻撃を受け、そのデバイスキーＤＫ_２が暴かれてしまったことがわかっている場合、図２に示したように、マスターキーＭＫの更新用のデータ（暗号化マスターキーＣ（ｊ，ｉ＋１））のうちの、カテゴリ番号２に対応する暗号化マスターキーＣ（２，ｉ＋１）の欄は空欄とされる。このようにして、デバイスキーＤＫが暴かれてしまったデバイスには、新たな世代のマスターキーＭＫ_i+１を付与しないことにより、デバイスキーＤＫ_２を持つデバイスを正当な利用権を有するグループからリボーク（排除）することができる。

図３のフローチャートを参照して、世代ｉのマスターキーＭＫ_iを世代ｉ＋１のマスターキーＭＫ_i+１に更新する際の情報再生装置の動作について説明する。ステップＳ３０１において、上述したようなマスターキーＭＫの更新用のデータが記録された記録媒体（光ディスク）１５０が、ユーザにより情報再生装置にセットされる。情報再生装置のデータ読み出し部１０５は、ステップＳ３０２において、セットされた光ディスクから、自分のカテゴリ番号ｊ（記憶しているデバイスキーＤＫ）に割り当てられている暗号化マスターキーＣ（ｊ，ｉ＋１）を読み出す。例えば、カテゴリ番号ｊが３である場合、暗号化マスターキーＣ（３，ｉ＋１）が読み出される。

このようにして読み出された暗号化マスターキーＣ（ｊ，ｉ＋１）は、ステップＳ３０３において、暗号文保持部１０２に記憶される。暗号文保持部１０２には、このようにして更新された暗号化マスターキーＣ（ｊ，ｉ＋１）のみが記憶される。

以上のようにして、暗号文保持部１０２に記憶された暗号化マスターキーＣ（ｊ，ｉ＋１）を用いて、光ディスク１５０に記録されているマスターキーＭＫに基づいて暗号化されたデータを再生する場合には、図４に示すように、マスターキー復号部１０３は、デバイスキー保持部１０１に保持されているデバイスキー：ＤＫ_jに基づいて、暗号文保持部１０２に記憶されている暗号化マスターキーＣ（ｊ，ｉ＋１）を復号することにより、マスターキーＭＫ_ｉ＋１を得る。そして、このマスターキーＭＫ_ｉ＋１に基づいて、記録媒体（光ディスク）１５０に記録されている暗号化されたデータが復号される。

このデータ再生処理手順を図５のフローチャートに示す。まず最初に、ステップＳ５００１において、情報再生装置のデータ読み出し部１０５は、セットされている記録媒体（光ディスク）１５０からデータを読み出す。ここで、記録媒体（光ディスク）１５０は、リードインエリアとデータエリアから構成されており、リードインエリアには、データエリアに記録されているデータのファイル名やディレクトリ情報などのＴＯＣ（Table Of Contents）などが記録されている。また、リードインエリアには、データエリアのデータがどの世代のマスターキーＭＫを用いて暗号化されているのかを示すデータ（世代情報）も記録されている。なお、この世代情報は、データを記録するときの暗号化に用いられたマスターキーＭＫの世代を表すので、以下、適宜、記録時世代情報という。

ステップＳ５０１では、データ読み出し部１０５において、リードインエリアのデータが読み出され、ステップＳ５０２に進む。ステップＳ５０２において、マスターキー復号部１０３は、暗号文保持部１０２を介して供給される、データ読み出し部１０５が読み出したデータから、データエリアのデータを暗号化するのに用いられたマスターキーＭＫの世代ｉを調べる。そして、ステップＳ５０３に進み、マスターキー復号部１０３は、調べたマスターキーＭＫの世代ｉのマスターキーＭＫ_ｉを作成する。

例えば、調べたマスターキーＭＫの世代が、最新世代の世代ｉ＋１である場合、マスターキー復号部１０３は、デバイスキー保持部１０１に保持されているデバイスキーＤＫを用いて、暗号文保持部１０２に記憶されている暗号化マスターキーＣ（ｊ，ｉ＋１）を復号することにより、マスターキーＭＫ_ｉ＋１を作成する。

また、調べたマスターキーＭＫの世代が、暗号文保持部１０２に保持されている以前の世代である場合、マスターキー復号部１０３は、暗号文保持部１０２に記憶されている暗号化マスターキーＣから、その世代のマスターキーＭＫを作成する。すなわち、マスターキー復号部１０３は、まず、上述したようにしてマスターキーＭＫ_i+１を復号する。さらに、マスターキー復号部１０３は、一方向性関数ｆを保持しており、その一方向性関数ｆに、マスターキーＭＫ_i+１を、そのマスターキーＭＫ_i+１の世代と、調べたマスターキーＭＫの世代との差に対応する回数だけ適用することにより、調べた世代のマスターキーＭＫを作成する。

例えば、暗号文保持部１０２に記憶されているマスターキーＭＫの世代が世代ｉ＋１であり、読み取られたマスターキーＭＫの世代が世代ｉ－１である場合、マスターキーＭＫ_i-１は、マスターキー復号部１０３において、一方向性関数ｆが２回用いられ、ｆ（ｆ（ＭＫ_i+１））が計算されることにより生成される。また、暗号文保持部１０２に記憶されているマスターキーＭＫの世代が世代ｉ＋１であり、読み取られたマスターキーＭＫの世代が世代ｉ－２である場合、マスターキーＭＫ_i-２は、一方向性関数ｆを３回用いて、ｆ（ｆ（ｆ（ＭＫ_i+１））））が計算されることにより生成される。

ここで、一方向性関数としては、例えば、ハッシュ(hash)関数を用いることができる。具体的には、例えば、ＭＤ５(Message Digest ５)や、ＳＨＡ－１(Secure Hash Algorithm - １)等を採用することができる。キーを発行するキー発行機関は、これらの一方向性関数を用いて自身の世代より前の世代を生成可能なマスターキーＭＫ_１，ＭＫ_２，・・・，ＭＫ_Ｎを、予め求めておく。すなわち、まず最初に、第Ｎ世代のマスターキーＭＫ_Ｎを設定し、そのマスターキーＭＫ_Ｎに、一方向性関数を１回ずつ適用しいくことで、それより前の世代のマスターキーＭＫ_Ｎ-１，ＭＫ_Ｎ-２，・・・，ＭＫ_１を順次生成しておく。そして、世代の小さい（前の）マスターキーＭＫ_１から順番に使用していく。なお、自身の世代より前の世代のマスターキーを生成するのに用いる一方向性関数は、全ての情報再生装置のマスターキー復号部１０３に設定されているものとする。

また、一方向性関数としては、例えば、公開鍵暗号技術を採用することも可能である。この場合、キー発行機関は、公開鍵暗号方式の秘密鍵を所有し、その秘

密鍵に対する公開鍵を、全ての情報再生装置に与えておく。そして、キー発行機関は、第１世代のマスターキーＭＫ_１を設定し、そのマスターキーＭＫ_１から使用していく。すなわち、キー発行機関は、第２世代以降のマスターキーＭＫ_iが必要になったら、その１世前のマスターキーＭＫ_i-１を、秘密鍵で変換することにより生成して使用する。この場合、キー発行機関は、一方向性関数を用いて、Ｎ世代のマスターキーを、予め生成しておく必要がない。また、この方法によれば、理論上は、無制限の世代のマスターキーを生成することができる。

なお、情報再生装置では、ある世代のマスターキーＭＫを有していれば、そのマスターキーＭＫを、公開鍵で変換することにより、その世代より前の世代のマスターキーを得ることができる。

以上のように、マスターキー復号部１０３は、最新世代のマスターキーＭＫの暗号化マスターキーＣを用いて、その世代より前の世代のマスターキーＭＫを作成できるので、暗号文保持部１０２は、最新世代のマスターキーＭＫの暗号化マスターキーＣのみを記憶していればよい。

ステップＳ５０３において、調べた世代のマスターキーＭＫが作成（復号）されたら、ステップＳ５０４において、データ読み出し部１０５は、記録媒体（光ディスク）１５０のデータエリアからデータを読み出す。さらに、ステップＳ５０４において、解読部１０４は、ステップＳ５０３で得られたマスターキーＭＫを用いて、データ読み出し部１０５が読み出したデータを解読（復号）する。解読されたデータは、例えば、そのデータが画像データである場合、ステップＳ５０５において、表示デバイスに出力され、表示される。

以上のように、自身の世代より前の世代を生成可能なマスターキーＭＫを、各デバイスが保持しているデバイスキーＤＫにより暗号化して配布することで、マスターキーＭＫを更新するようにしたので、インタオペラビリティを保ったまま、マスターキーＭＫを更新したり、暴かれたデバイスキーＤＫを保持するデバイスを排除することが可能となる。また、各デバイスは、一方向性関数ｆを用いることにより、最新世代のマスターキーＭＫを保持していれば、指定のマスターキーＭＫを作成できるので、デバイスが所持しなくてはならないメモリの容量を削減することが可能となる。

ここで、情報再生装置においては、データの復号に用いられたマスターキーＭＫは、その復号の終了後に廃棄される。そして、マスターキーＭＫは、再び必要となったときに、暗号化マスターキーＣを、デバイスキーＤＫに基づいて復号することで生成される。情報再生装置では、このようにして、暗号化されていないマスターキーＭＫが放置されることによる秘匿性の劣化が防止されるようになっている。

さらに、上述の場合においては、暗号文保持部１０２に、更新後の世代の暗号化マスターキーＣのみを記憶させるようにしたが、暗号文保持部１０２には、その他、各世代の暗号化マスターキーＣを記憶させるようにしてもよい。この場合、各世代のマスターキーＭＫを計算せずに済み、その分の処理負担が軽減される。

なお、上述のように、一方向性関数を用いて自身の世代より前の世代を生成可能なマスターキーＭＫ_１，ＭＫ_２，・・・，ＭＫ_Ｎについては、その逆に、自身の世代より後の世代を生成することはできないから、古い世代のマスターキーＭＫから、新しい世代のマスターキーＭＫが生成されることによって、データが不正に復号されることはない。

ところで、上述した構成においては、マスターキーＭＫを更新することで、その更新後のマスターキーＭＫに基づいて暗号化されたデータは保護することが可能となるが、更新前のマスターキーＭＫに基づいて暗号化されたデータの保護には、やや課題が残る。すなわち、上述のようなマスターキーの更新処理方法は、データを、マスターキーで暗号化して記録する記録装置にも適用可能であり、記録装置において、前の世代のマスターキーＭＫが用いられた暗号化がなされてしまうと、上述のように、攻撃者から攻撃を受け、新たな世代のマスターキーＭＫが与えられない情報再生装置（即ちリボークされるべきデバイス）であっても、その前の世代のマスターキーＭＫを有していれば、記録媒体からの再生が可能となる。

したがって、前の世代のマスターキーＭＫを用いて暗号化処理を行っている記録装置、即ち、マスターキーＭＫを更新しない、あるいはできない記録装置が長時間使用されると、その間に、不正な情報再生装置、即ち、新たな世代のマスターキーＭＫが与えられない情報再生装置によって、データが復号されてしまうこ

とになる。

[２．厳格なマスターキー世代管理を可能とした構成]

(２．１．記録再生装置構成)

上述の問題を解決する構成を備えた記録再生装置６００の一実施形態の構成例を図６に示す。バス６１０は、ディジタルＩ／Ｆ(Interface)６２０，ＭＰＥＧ(Moving Picture Experts Group)コーデック６３０、例えば暗号化／復号ＬＳＩ(Large Scale Integrated Curcuit)によって構成される暗号処理手段６５０、ＣＰＵ(Central Processing Unit)６７０、メモリ６８０、記録媒体Ｉ／Ｆ６９０、及びユーザＩ／Ｆ６６０を相互に接続している。

ディジタルＩ／Ｆ６２０は、外部から供給されるコンテンツとしてのディジタル信号を受信し、バス６１０上に出力するとともに、バス６１０上のディジタル信号を受信し、外部に出力する。ＭＰＥＧコーデック６３０は、バス６１０を介して供給される、ＭＰＥＧ符号化されたデータを、ＭＰＥＧデコードし、Ａ／Ｄ，Ｄ／Ａコンバータ６３５に出力するとともに、Ａ／Ｄ，Ｄ／Ａコンバータ６３５から供給されるディジタル信号をＭＰＥＧエンコードしてバス６１０上に出力する。

Ａ／Ｄ，Ｄ／Ａコンバータ６３５は、ＭＰＥＧコーデック６３０からのＭＰＥＧデコードされたディジタル信号を、Ｄ／Ａ(Digital Analog)変換することで、アナログ信号とし、アナログＩ／Ｆ６４０に供給するとともに、アナログＩ／Ｆ６４０からのアナログ信号を、Ａ／Ｄ(Analog Digital)変換することで、ディジタル信号とし、ＭＰＥＧコーデック６３０に出力する。アナログＩ／Ｆ３５は、外部から供給されるコンテンツとしてのアナログ信号を受信し、Ａ／Ｄ，Ｄ／Ａコンバータ６３５に出力するとともに、Ａ／Ｄ，Ｄ／Ａコンバータ６３５からのアナログ信号を、外部に出力するようになっている。

暗号処理手段６５０は、例えば、１チップのＬＳＩ(Large Scale Integrated Curcuit)で構成され、バス６１０を介して供給されるコンテンツとしてのディジタル信号を暗号化し、又は復号し、バス６１０上に出力する構成を持つ。なお、暗号処理手段６５０は１チップＬＳＩに限らず、各種のソフトウェア又はハードウェアを組み合わせた構成によって実現することも可能である。ソフトウェア構

成による処理手段としての構成については後段で説明する。

ＣＰＵ６７０は、メモリ６８０に記憶されたプログラムを実行することで、ＭＰＥＧコーデック６３０や暗号処理手段６５０等を制御するとともに、各種の処理を行う。メモリ６８０は、例えば、不揮発性メモリで、ＣＰＵ６７０が実行するプログラムや、ＣＰＵ６７０の動作上必要なデータを記憶する。記録媒体Ｉ／Ｆ６９０は、例えば、光ディスク等の記録媒体２００からディジタルデータを読み出し（再生し）、バス６１０上に出力するとともに、バス６１０を介して供給されるディジタルデータを、記録媒体２００に供給して記録する構成となっている。

ユーザＩ／Ｆ６６０は、図示しない表示部や入力部を備え、ユーザに情報を提示したりユーザからの指示を受け取ってバス６１０に出力したりする。

（２．２．暗号処理部構成）

次に、図７を用いて、図６に示す暗号処理手段６５０（ｅｘ．暗号化／復号ＬＳＩ）の詳細構成について説明する。なお、図中、図１の情報再生装置における場合と対応する部分については、同一の符号を付してあり、以下では、その説明は、適宜省略する。

エンコーダ７０１は、マスターキー復号部１０３が出力するマスターキーＭＫに基づいて、バス６１０を介して供給される平文のコンテンツ（平文コンテンツ）を暗号化することにより暗号文（暗号化コンテンツ）とし、その暗号化コンテンツを、バス６１０上に出力する。デコーダ７０２は、マスターキー復号部１０３が出力するマスターキーＭＫに基づいて、バス６１０を介して供給される暗号化コンテンツを復号することにより平文コンテンツとし、その平文コンテンツを、バス６１０上に出力する。マスターキー更新部７０３は、暗号文保持部１０２に記憶されたマスターキーＭＫの更新を制御する。

（２．３．キーテーブル・フォーマット）

次に、図６の記録再生装置６００が、記録再生の対象とする記録媒体２００のフォーマットの例を図８に示す。図８に示す実施形態は、図２における記録媒体（光ディスク）１５０と同様の、世代ｉのマスターキーＭＫ_iを、世代ｉ＋１のマスターキーＭＫ_i+1に更新するキーテーブルを格納した記録媒体２００を示し

ており、記録媒体２００には、上述の光ディスク１５０における場合と同様の、カテゴリ番号ｊと暗号化マスターキーＣ（ｊ，ｉ＋１）とが、それぞれ対応付けられたテーブル（キーテーブル）が記録されている。さらに、記録媒体２００には、この記録媒体２００に対するデータの記録及び再生に必要なマスターキーＭＫの最小の世代を表す世代情報Generation#nが記録されている。ここで、この世代情報Generation#nは、例えば、記録媒体２００の製造時に、予め記録されるものであり、上述の記録時世代情報と区別するために、以下、適宜、プレ記録世代情報（Pre Recording Generation#n）という。

この図８に示す記録媒体２００に対するデータの記録及び再生に必要なマスターキーＭＫの最小の世代は世代番号：ｎである。世代番号：ｎは例えばシーケンシャルな世代番号として付与される。記録再生装置６００が自身の記憶手段に格納しているマスターキーの世代がｎより以前である場合は、図８に示す記録媒体２００に対する記録、及び記録媒体２００からの再生が拒否される。

図８に示す記録媒体２００は、各記録再生装置に格納したデバイスキーＤＫによってキーテーブルに格納された暗号化マスターキーＣ（ｉ＋１）を復号処理することによってマスターキーＭＫ_ｉ＋１を取得可能とした記録媒体である。

なお、キーテーブルは全ての記録媒体に格納されるものではなく、単に世代番号（プレ記録世代番号）のみが記録された記録媒体２００を記録再生装置６００に装着して記録あるいは再生を実行する場合には、世代番号（プレ記録世代番号）と各記録再生装置に格納されたマスターキーの世代番号の比較処理が記録再生装置６００において実行され、記録再生装置６００が自身の記憶手段の格納マスターキーの世代が記録媒体の世代番号（プレ記録世代番号）ｎより古いものである場合は、図８に示す記録媒体２００に対する記録、及び記録媒体２００からの再生が行えない。

図８に示す記録媒体２００に対するデータの記録及び再生に必要なマスターキーＭＫの最小の世代はｎである。記録再生装置６００が自身の記憶手段に格納しているマスターキーの世代がｎと同一か、より新しい記録再生装置は、記録媒体２００への記録が行える。しかし、記録再生装置６００が自身の記憶手段に格納しているマスターキーの世代がｎより古い場合には、記録媒体２００へのデータ

の記録は許されず、たとえ不正装置が古いマスターキーを用いて記録を行ったとしても、正しい再生装置はこのデータを再生しない。また、記録媒体２００に正当に記録されるデータは必ずｎと同一かより新しい世代のマスターキーに基づいて暗号化されて記録されるため、記録再生装置６００が自身の記憶手段に格納しているマスターキーの世代がｎより古い場合には、この記録再生装置は記録媒体のデータを復号できない（再生できない）ことになる。

なお、キーテーブル及びプレ記録世代情報Generation#nは、記録媒体２００において、その書き換えが不可能な領域（書き換え不可の領域）としての、例えば、リードインエリアに記録されており、これにより、キーテーブル及びプレ記録世代情報Generation#nが不正に書き換えられることを防止するようになっている。

図８に示す記録媒体２００に対するデータの記録は、その記録媒体２００におけるプレ記録世代情報が表す世代以後の世代のマスターキーＭＫを有していなければ行うことができない（許可されない）ように、装置の設計を行う。したがって、ある世代ｎを表すプレ記録世代情報Generation#nが記録された記録媒体２００が流通することで、記録媒体２００に対する記録を行う記録装置や、その記録再生が可能な図６の記録再生装置におけるマスターキーの更新が促進され、これにより、前の世代のマスターキーＭＫを用いている記録装置や記録再生装置が減少していき、その結果、不正なデータの復号が防止される。

すなわち、プレ記録世代情報が記録されていない、例えば前述の図４を用いて説明した記録媒体（光ディスク）１５０に対しては、上述のように、マスターキーを更新していない記録装置によって、データの記録が可能であり、そのようにしてデータが記録された光ディスク１５０は、マスターキーを更新していない情報再生装置で再生することができてしまうが、一方、プレ記録世代情報が記録されている図８を用いて説明した記録媒体２００に対しては、プレ記録世代情報が表す世代以後の世代のマスターキーＭＫを有していなければ、データの記録が許可されない。すなわち、記録媒体２００へのデータの記録を行うには、そこに記録されているプレ記録世代情報が表す世代以後の世代のマスターキーＭＫが必要となるから、マスターキーを更新していない記録装置によるデータの記録が防止される。

なお、本実施の形態では、記録媒体２００に記録されているキーテーブルにおけるマスターキーの世代が、プレ記録世代情報Generation#nとして記録されているものとする。但し、記録媒体２００に記録されているキーテーブルにおけるマスターキーの世代と、プレ記録世代情報Generation#nが表す世代ｎとは、必ずしも一致している必要はない。

（２．４．マスターキー更新処理）

次に、図９乃至１２を参照して、図６の記録再生装置の各種処理について説明する。まず最初に、図９のフローチャートを参照して、データの記録又は再生のために、記録媒体２００が、記録再生装置にセットされたとき等に行われるマスターキー更新処理について説明する。

記録媒体２００が、記録再生装置にセットされると、まず最初に、ステップＳ９０１において、記録媒体Ｉ／Ｆ６９０（図６参照）は、記録媒体２００から、キーテーブル世代情報Generation#ｉ+１を読み出し、暗号処理手段６５０のマスターキー更新部７０３（図７参照）に供給する。マスターキー更新部７０３は、暗号文保持部１０２が記憶している暗号化マスターキーＣを読み出し、ステップＳ９０２において、その暗号化マスターキーの世代と、キーテーブル世代情報Generation#ｉ+１が表す世代ｉ＋１とを比較して、その世代の前後を判定する。

ステップＳ９０２において、キーテーブル世代情報Generation#ｉ+１が表す世代ｉ＋１の方が、暗号文保持部１０２に記憶された暗号化マスターキーＣの世代よりも後でない（新しくない）と判定された場合、即ち、暗号文保持部１０２に記憶された暗号化マスターキーＣの世代が、キーテーブル世代情報Generation#ｉ+１が表す世代ｉ＋１と同一か、又は後の場合、ステップＳ９０３乃至Ｓ９０５をスキップして、マスターキー更新処理を終了する。

すなわち、この場合、暗号文保持部１０２に記憶されたマスターキーＭＫ（暗号化マスターキーＣ）の更新は行う必要がないので、その更新は行われない。

一方、ステップＳ９０２において、キーテーブル世代情報Generation#ｉ+１が表す世代ｉ＋１の方が、暗号文保持部１０２に記憶された暗号化マスターキーＣの世代よりも後である（新しい）と判定された場合、即ち、暗号文保持部１０２に記憶された暗号化マスターキーＣの世代が、キーテーブル世代情報Generation

#i+1が表す世代ｉ＋１よりも前の世代である場合、ステップＳ９０３に進み、記録媒体Ｉ／Ｆ６９０は、記録媒体２００（図８参照）から、キーテーブルを読み出し、暗号処理手段６５０（図７参照）のマスターキー更新部７０３に供給する。

マスターキー更新部７０３では、ステップＳ９０４において、キーテーブル、自身のデバイス番号ｊに割り当てられた暗号化マスターキーＣが存在するかどうかが判定され、存在しないと判定された場合、ステップＳ９０５をスキップして、マスターキー更新処理を終了する。

すなわち、例えば、図２を参照して説明したように、記録再生装置が、攻撃者から攻撃を受け、そのデバイスキーＤＫ_jが暴かれてしまったことがわかっている場合には、キーテーブルにおけるカテゴリ番号ｊに対応する暗号化マスターキーＣ（ｊ，ｉ＋１）の欄は空欄とされるため、マスターキーＭＫの更新は行われない（行うことができない）。

一方、ステップＳ９０４において、キーテーブルに、自身のデバイス番号ｊに割り当てられた暗号化マスターキーＣが存在すると判定された場合、ステップＳ９０５に進み、マスターキー更新部７０３は、その暗号化マスターキーＣを、暗号文保持部１０２に供給し、そこに記憶されている暗号化マスターキーに替えて記憶させ、マスターキー更新処理を終了する。

（２．５．コンテンツ記録処理）

次に、図１０のフローチャートを参照して、記録媒体２００に対してデータの記録が行われる場合の、記録再生装置の処理について説明する。

まず最初に、ステップＳ１００１において、記録媒体Ｉ／Ｆ６９０は、記録媒体２００から、プレ記録世代情報Generation#nを読み出し、ＣＰＵ６７０に供給する。ＣＰＵ６７０は、暗号処理手段６５０（図７）の暗号文保持部１０２が記憶している暗号化マスターキーＣの世代を認識し、ステップＳ１００２において、その暗号化マスターキーの世代と、プレ記録世代情報Generation#nが表す世代ｎとを比較して、その世代の前後を判定する。

ステップＳ１００２において、暗号文保持部１０２に記憶された暗号化マスターキーＣの世代が、プレ記録世代情報Generation#nが表す世代ｎ以後でないと判

定された場合、即ち、暗号文保持部１０２に記憶された暗号化マスターキーＣの世代が、プレ記録世代情報Generation#nが表す世代ｎよりも古い世代である場合、ステップＳ１００５に進む。

一方、ステップＳ１００２において、暗号文保持部１０２に記憶された暗号化マスターキーＣの世代が、プレ記録世代情報Generation#nが表す世代ｎ以後であると判定された場合、即ち、暗号文保持部１０２に記憶された暗号化マスターキーＣの世代が、プレ記録世代情報Generation#nが表す世代ｎと同一か、又はそれよりも新しい場合、ステップＳ１００３に進み、ＣＰＵ６７０は、記録媒体Ｉ／Ｆ６９０を制御することにより、暗号文保持部１０２に記憶された暗号化マスターキーＣの世代を表す世代情報を、記録時世代情報とし、記録媒体２００（図８参照）に記録させる。

そして、記録媒体２００に記録すべきコンテンツが、記録再生装置に入力されると、ステップＳ１００４において、そのコンテンツは、暗号処理手段６５０で暗号化され、バス６１０を介して、記録媒体Ｉ／Ｆ６９０に供給される。

すなわち、記録媒体２００に記録すべきコンテンツとしてのディジタル信号が、ディジタルＩ／Ｆ６２０に供給されると、ディジタルＩ／Ｆ６２０は、そのディジタル信号を、バス６１０を介して、暗号処理手段６５０（図７参照）のエンコーダ７０１に供給する。また、記録媒体２００に記録すべきコンテンツとしてのアナログ信号が、アナログＩ／Ｆ６４０に供給されると、そのアナログ信号は、コンバータ６３５を介することにより、ディジタル信号とされ、ＭＰＥＧコーデック６３０に供給される。そして、ＭＰＥＧコーデック６３０において、コンバータ６３５からのディジタル信号がＭＰＥＧエンコードされ、バス６１０を介して、暗号処理手段６５０のエンコーダ７０１に供給される。

暗号処理手段６５０では、マスターキー復号部１０３において、暗号文保持部１０２に記憶されている暗号化マスターキーＣが、デバイスキー保持部１０１に記憶されているデバイスキーＤＫに基づいて、マスターキーＭＫに復号され、エンコーダ７０１に供給される。エンコーダ７０１では、マスターキー復号部１０３からのマスターキーＭＫを用いて、そこに供給される平文のディジタル信号（コンテンツ）が暗号化され、その結果得られる暗号化コンテンツが、バス６１

０を介して、記録媒体Ｉ／Ｆ６９０に供給される。

さらに、ステップＳ１００４では、記録媒体Ｉ／Ｆ６９０において、暗号処理手段６５０からの暗号化コンテンツが、記録媒体２００に供給されて記録され、処理を終了する。

なお、例えば、記録媒体２００が、光ディスク等のディスク形状の記録媒体である場合には、記録時世代情報は、例えば、図１１に示すように、セクタのセクタヘッダ等に記録される。すなわち、セクタは、セクタヘッダとユーザデータ部とから構成され、記録時世代情報は、その記録時世代情報が表す世代のマスターキーＭＫで暗号化された暗号化コンテンツが、ユーザデータ部に記録されるセクタのセクタヘッダに記録される。ここで、このような世代情報の記録方法については、本件出願人が先に提案している特願平１０－３５２９７５号に、その詳細を記載している。

また、記録媒体２００に対して、暗号化コンテンツを、ファイルとして記録する場合には、記録時世代情報は、そのファイルと対応付けて管理することができるような形で、記録媒体２００に記録することができる。

ここで、上述の場合には、暗号文保持部１０２に記憶された世代のマスターキーを用いて、コンテンツを暗号化して記録するようにしたが、その他、例えば、暗号文保持部１０２に記録された世代のマスターキーから、記録媒体２００に記録されているプレ記録世代情報が表す世代のマスターキーを生成し、そのマスターキーを用いて、コンテンツを暗号化して記録することも可能である。この場合、記録媒体２００に記録されるコンテンツの暗号化に用いられるマスターキーの世代は、その記録媒体２００に記録されているプレ記録世代情報が表す世代に、必ず一致するから、記録時世代情報は、記録媒体２００に記録する必要がなくなる。

一方、ステップＳ１００５に進んだ場合、暗号文保持部１０２に記憶された暗号化マスターキーＣの世代が、プレ記録世代情報Generation#nが表す世代ｎよりも古い世代である場合には、記録媒体２００へのデータの記録は許可されない（行うことができない）。

このため、ステップＳ１００５では、ユーザＩ／Ｆ６６０を介して、ユーザに対し、より新しい世代のマスターキーへの更新を促すメッセージを表示、又は音

声出力等により、警告音、警告表示の出力を実行して処理を終了する。

これにより、ユーザがこのメッセージに従って、例えば、機器メーカーのサービスステーションに機器を持ち込んでマスターキーを更新したり、下記の実施例に述べる方法でマスターキーを更新することによって、次回以降、この記録媒体２００へのデータの記録が行えるようになる。

（２．６．コンテンツ再生処理）

次に、図１２のフローチャートを参照して、記録媒体２００からのデータの再生が行われる場合の、記録再生装置の動作について説明する。

まず最初に、ステップＳ１２０１において、記録媒体Ｉ／Ｆ６９０は、記録媒体２００から、プレ記録世代情報Generation#nを読み出し、ＣＰＵ６７０に供給する。さらに、記録媒体Ｉ／Ｆ６９０は、ステップＳ１２０２に進み、再生しようとしているコンテンツ（データ）の暗号化に用いられたマスターキーＭＫの世代情報（記録時世代情報）を、記録媒体２００から読み出し、ＣＰＵ６７０に供給する。

ＣＰＵ６７０は、ステップＳ１２０３において、記録媒体Ｉ／Ｆ６９０からのプレ記録世代情報Generation#nが表す世代ｎと、記録時世代情報が表す世代ｍとを比較し、その世代の前後を判定する。

ステップＳ１２０３において、記録時世代情報が表す世代ｍが、プレ記録世代情報Generation#nが表す世代ｎ以後でないと判定された場合、即ち、記録時世代情報が表す世代ｍが、プレ記録世代情報Generation#nが表す世代ｎよりも古い世代である場合、ステップＳ１２０４乃至Ｓ１２０６をスキップして、処理を終了する。

したがって、記録媒体２００に記録されたコンテンツが、プレ記録世代情報Genaration#nが表す世代ｎよりも古い世代のマスターキーＭＫに基づいて暗号化されたものである場合には、その再生は行われない（再生は許可されない）。

すなわち、この場合は、不正が発覚して、最新の世代のマスターキーが与えられなくなった不正な記録装置で、古い世代のマスターキーに基づいて、データが暗号化され、記録媒体２００に記録された場合に該当するから、そのような不正な装置によってデータが記録された記録媒体２００の再生は行われないようにな

っており、これにより、不正な記録装置の使用を排除することができるようになっている。

一方、ステップＳ１２０３において、記録時世代情報が表す世代ｍが、プレ記録世代情報Generation#nが表す世代ｎ以後であると判定された場合、即ち、記録時世代情報が表す世代ｍが、プレ記録世代情報Generation#nが表す世代ｎと同一か、又は新しい世代であり、従って、記録媒体２００に記録されたコンテンツが、プレ記録世代情報Generation#nが表す世代ｎ以後の世代のマスターキーＭＫに基づいて暗号化されたものである場合には、ステップＳ１２０４に進み、ＣＰＵ６７０は、暗号処理部６５０（図７）の暗号文保持部１０２が記憶している暗号化マスターキーＣの世代を認識し、その暗号化マスターキーの世代と、記録時世代情報が表す世代ｍを比較して、その世代の前後を判定する。

ステップＳ１２０４において、暗号文保持部１０２に記憶された暗号化マスターキーＣの世代が、記録時世代情報が表す世代ｍ以後でないと判定された場合、即ち、暗号文保持部１０２に記憶された暗号化マスターキーＣの世代が、記録時世代情報が表す世代ｍよりも古い世代である場合、ステップＳ１２０７に進む。

一方、ステップＳ１２０４において、暗号文保持部１０２に記憶された暗号化マスターキーＣの世代が、記録時世代情報が表す世代ｍ以後であると判定された場合、即ち、暗号文保持部１０２に記憶された暗号化マスターキーＣの世代が、記録時世代情報が表す世代ｍと同一か、又はそれよりも新しい場合、ステップＳ１２０５に進み、暗号処理手段６５０（図７参照）のマスターキー復号部１０３において、暗号文保持部１０２に記憶されている暗号化マスターキーＣが、デバイスキー保持部１０１に記憶されているデバイスキーＤＫに基づいて、マスターキーＭＫに復号される。さらに、マスターキー復号部１０３は、その復号したマスターキーＭＫの世代が、記録時世代情報が表す世代ｍよりも新しい場合には、上述したようにして、復号したマスターキーＭＫから、記録時世代情報が表す世代ｍのマスターキーＭＫを生成し、デコーダ７０２に供給する。

そして、ステップＳ１２０６に進み、記録媒体Ｉ／Ｆ６９０は、記録媒体２００から暗号化コンテンツを読み出し、バス６１０を介して、暗号処理手段６５０に供給する。さらに、ステップＳ１２０６では、暗号処理手段６５０のデコーダ

７０２において、記録媒体２００からの暗号化コンテンツが、ステップＳ１２０５で得られたマスターキーＭＫに基づいて復号され、処理を終了する。

以上のようにして復号されたコンテンツは、バス６１０及びディジタルＩ／Ｆ６２０を介して、外部に出力される。あるいは、また、コンテンツは、ＭＰＥＧコーデック６３０においてＭＰＥＧデコードされ、コンバータ６３５を介することにより、アナログ信号とされて、アナログＩ／Ｆ６４０を介して、外部に出力される。

一方、ステップＳ１２０７では、暗号文保持部１０２に記憶された暗号化マスターキーＣの世代が、記録時世代情報が表す世代ｍよりも古い世代であるので、記録媒体２００からのデータ再生は許可されない。すなわち、暗号化マスターキーＣの世代が、記録時世代情報が表す世代ｍよりも古い世代である場合には、上述したように、暗号化マスターキーＣから得られるマスターキーＭＫから、その世代よりも新しい世代ｍのマスターキーＭＫを生成することはできないため、記録媒体２００からのデータの再生は行われない（行うことができない）。

このため、ステップＳ１２０７では、ユーザＩ／Ｆ６６０を介して、ユーザに対し、より新しい世代のマスターキーへの更新を促すメッセージを表示して処理を終了する。すなわち、ユーザＩ／Ｆ６６０を介して、ユーザに対し、より新しい世代のマスターキーへの更新を促すメッセージを表示、又は音声出力等により、警告音、警告表示の出力を実行して処理を終了する。

これにより、ユーザがこのメッセージに従って、例えば、機器メーカーのサービスステーションに機器を持ち込んでマスターキーを更新したり、下記の実施例に述べる方法でマスターキーを更新することによって、次回以降、この記録媒体２００からのデータの再生が行えるようになる。

以上のように、記録時世代情報が表す世代が、プレ記録世代情報が表す世代以後の世代でない場合には、再生を行うことができないようにしたので、マスターキーの更新を、いわば強制することができ、これにより、不正な装置により記録が行われた記録媒体の流通を、間接的に排除することができる。

また、機器が最新のマスターキーを記憶していないためにある記録媒体へのデータの記録又は再生が行えない場合には、ユーザにマスターキーの更新を促すメ

ッセージを表示し、システム全体でのマスターキーの更新作業をさらに加速することができる。

［３．その他の実施例］

（３．１．ＩＣカードによるマスターキー更新構成）

次に、本発明を適用した記録再生装置の別の実施例の形態の構成例を図１３に示す。

図１３の各構成要素の大部分は図６と同様であり、説明を省略する。図１３において、バス６１０にはＩＣ（Integrated Curcuit）カードＩ／Ｆ１３０１が接続されている。ＩＣカードＩ／Ｆ１３０１は、記録再生装置に着脱可能なＩＣカード１３０２とデータをやりとりするためのインタフェースである。

記録媒体２００が、この記録再生装置にセットされたとき等に行われるマスターキーの更新処理は、図９と同様である。

次に、図１４のフローチャートを参照して、記録媒体２００に対するデータの記録が行われる場合の、記録再生装置の動作について説明する。

図１４において、ステップＳ１４０１乃至Ｓ１４０５の処理は、図１０のステップＳ１００１乃至Ｓ１００５の各処理と同様であるため、説明を省略する。但し、ステップＳ１４０５においては、ユーザに対してマスターキーの更新を促すメッセージを表示した後、ステップＳ１４０６に進む。すなわち、ユーザＩ／Ｆ６６０を介して、ユーザに対し、より新しい世代のマスターキーへの更新を促すメッセージを表示、又は音声出力等により、警告音、警告表示の出力を実行してステップＳ１４０６に進む。

ステップＳ１４０６では、ＩＣカード１３０２がユーザによって装置に装着されるのを待ち、そしてＩＣカード１３０２を用いてマスターキーの更新を行う。すなわち、ＩＣカード１３０２には、図８を用いて説明した記録媒体２００に記録されているのと同様のキーテーブルが格納されており、これを上述の方法を用いて処理することにより、最新世代の暗号化マスターキーを記録再生装置が得ることが可能である。

上記例では、ＩＣカード１３０２には、図８を用いて説明した記録媒体２００に記録されているのと同様のキーテーブルが格納されているとしたが、これは以

下のようなものであってもよい。

すなわち、記録再生機器のメモリ６８０には個々の記録再生機器を識別するための識別情報（機器ＩＤ）と、個々の機器ＩＤに対応するデバイスキーが格納されており、ＩＣカード１３０２には、機器ＩＤと、最新世代のマスターキーを個々の機器ＩＤに対応するデバイスキーで暗号化した暗号化マスターキーが格納されている。これを記録媒体２００に格納されているキーテーブルと同様に取り扱うことによって、最新世代の暗号化マスターキーを記録再生装置が入手することが可能である。

ＩＣカードはキー発行機関が、個々のユーザ毎に個々のデータを格納して郵送するなどの方法がとりやすいため、このようにＩＣカードを用いることにより、よりきめこまかな鍵の管理が行え、記録媒体の記録容量をキーテーブルで消費してしまうことがないという利点を持つ。

次に、ステップＳ１４０７では、ステップＳ１４０６で必要な世代の暗号化マスターキーがＩＣカード５１を介して取得できたかどうかの検査を行う。

もし必要な世代の暗号化マスターキーが取得できていれば、ステップＳ１４０３に進み、最終的に記録媒体２００へのデータの記録を行う。

必要な世代の暗号化マスターキーが取得できなければ、データの記録は行わずに処理を終了する。なお、この際に、必要な世代の暗号化マスターキーが取得できなかった旨のメッセージをユーザに対して表示してもよい。

次に、図１５のフローチャートを参照して、記録媒体２００に記録されたデータの再生が行われる場合の、記録再生装置の動作について説明する。

図１５において、ステップＳ１５０１乃至Ｓ１５０７の処理は、図１２のステップＳ１２０１乃至Ｓ１２０７の各処理と同様であるため、説明を省略する。但し、ステップＳ１５０７においては、ユーザに対してマスターキーの更新を促すメッセージを表示した後、ステップＳ１５０８に進む。すなわち、ユーザＩ／Ｆ６６０を介して、ユーザに対し、より新しい世代のマスターキーへの更新を促すメッセージを表示、又は音声出力等により、警告音、警告表示の出力を実行してステップＳ１５０８に進む。

ステップＳ１５０８では、図１４のステップＳ１４０６と同様にして、必要な

世代の暗号化マスターキーをＩＣカード５１から取得する。そして、ステップＳ１５０９に進む。

ステップＳ１５０９では、ステップＳ１５０８で必要な世代の暗号化マスターキーを取得できたか否かの検査を行う。

もし必要な世代の暗号化マスターキーが取得できていれば、ステップＳ１５０５に進み、最終的に記録媒体２００からのデータの再生を行う。

必要な世代の暗号化マスターキーが取得できなければ、データの記録は行わずに処理を終了する。なお、この際に、必要な世代の暗号化マスターキーが取得できなかった旨のメッセージをユーザに対して表示してもよい。

（３．２．モデムを介するマスターキー更新構成）

次に、本発明を適用した記録再生装置の別の実施例の形態の構成例を図１６に示す。

図１６の記録再生装置１６００の各構成要素の大部分は図６と同様であり、説明を省略するが、メモリ６８０には、記録再生装置固有の識別情報（機器ＩＤ）と、機器ＩＤ毎に固有の、共通鍵暗号系の暗号鍵又は、公開鍵暗号系の秘密鍵と公開鍵証明書などが格納されている。

図１６において、バス６１０にはモデム１６０１が接続されており、モデム１６０１は電話回線と接続されている。

次に、図１７のフローチャートを参照して、図１６の構成を有する記録再生装置１６００における記録媒体２００に対するデータの記録が行われる場合の、記録再生装置１６００の動作について説明する。

図１７において、ステップＳ１７０１乃至Ｓ１７０４の処理は、図１０のステップＳ１００１乃至Ｓ１００４の各処理と同様であるため、説明を省略する。

ステップＳ１７０２において、自身が格納する暗号化マスターキーの世代が、プレ記録世代情報よりも古いと判定された場合、ステップＳ１７０５において、記録再生装置はモデム１６０１を使用してキー発行機関と電話回線を介してリンクを張り、キー発行機関が送信した最新世代の暗号化マスタキーを受信して取得する。

なお、この際に、記録再生装置とキー発行機関が互いに相手の正当性を確認す

るために、相互認証のプロトコルを実行してもよい。相互認証のプロトコルの例としては、ISO/IEC 9798-2 に代表される、共通鍵暗号を用いるもの、ISO/IEC 9798-3に代表される、公開鍵暗号を用いるもの、ISO/IEC 9798-4 に代表される、暗号学的チェック関数を用いるものなどが挙げられる。

図１８は、暗号学的チェック関数を用いた相互認証及び暗号鍵共有のための方法のひとつを本実施例に用いたものである。

図１８において、記録再生機器（Device B と表す）は、固有の機器ＩＤ：ＩＤ_Bと、秘密鍵ＤＫ_Bを格納している。またキー発行機関Ａは、それぞれの機器の機器ＩＤ と、それぞれの機器ＩＤに対応する秘密鍵のテーブルを保存している。

まず、記録再生装置は乱数Ｒ_Bを発生し、ＩＤ_Bとともにキー発行機関に送る。なお、図１８における記号「||」は連結を表している。

次にキー発行機関は、乱数Ｒ_A、Ｓ_Aを生成し、Ｒ_A,Ｓ_A,ＩＤ_AとともにＭＡＣ(ＤＫ_B, Ｒ_A || Ｒ_B || Ｓ_A)を記録再生装置に送る。ＩＤ_Aはキー発行機関を表す識別情報であり、ＭＡＣ(ＤＫ_B, Ｒ_A || Ｒ_B || Ｓ_A)は、暗号学的チェック関数に鍵として ＤＫ_B を、データとして Ｒ_A || Ｒ_B || Ｓ_Aを入力することを表す。暗号学的チェック関数は、ISO/IEC 9797 に示されているように、FIPS 46-2 のデータ暗号化規格 (Data Encryption Standard, DES) を用いて構成することが可能である。またこの際使用する ＤＫ_Bは格納されているテーブルからＩＤ_Bを検索キーとして検索してくる。

記録再生装置は、受信したデータを用いて自分でもＭＡＣ(ＤＫ_B, Ｒ_A || Ｒ_B || Ｓ_A)を計算し、これが受信したものと一致するかを検査する。一致すれば、キー発行機関が正当なものとして認め、処理を続けるが、一致しなければキー発行機関が不正なものと判断して処理を中止する。

次に記録再生装置は乱数Ｓ_Bを生成し、これとＭＡＣ(ＤＫ_B, Ｒ_B || Ｒ_A || Ｓ_B)をキー発行機関に送る。

キー発行機関も受信したデータを用いて自分でＭＡＣ(ＤＫ_B, Ｒ_B || Ｒ_A || Ｓ_B)を計算し、受信したものと一致するかを確認する。一致すれば、記録再生装置が正当なものとして認め、処理を続けるが、一致しなければ記録再生装置が不正なものと判断して処理を中止する。

最後に、双方がＭＡＣ(ＤＫ_B, Ｓ_A || Ｓ_B)を計算し、これをそのセッションにおけるセッションキーとして使用する。

上記のようにすることにより、キー発行機関と記録再生装置は互いの正当性を検査することができ、またセッションキーを安全に共有することができたので、例えば、このセッションキーを鍵として、最新世代のマスターキーをＤＥＳなどで暗号化してキー発行機関が記録再生機器に安全に送信することが可能となる。

図１９は、公開鍵暗号を用いた認証技術を本実施例に適用したものである。

図１９において、キー発行機関Ａ及び記録再生装置Ｂは、それぞれ自分の識別情報であるＩＤと、自分の公開鍵証明書、及びリボケーションリスト又はレジストレーションリストを持っている。公開鍵証明書は、図２０に示すように、そのエンティティのＩＤと、公開鍵に対し、センタ（キー発行機関）が署名を施したデータである。

リボケーションリストは、不正者リストあるいはブラックリストとも呼ばれ、図２１に示すように、その装置の秘密鍵が露呈してしまったもののＩＤがリストアップされ、単調増加するバージョンナンバとともにセンタ（キー発行機関）のディジタル署名が施されたものである。

これに対し、レジストレーションリストは、正当者リストあるいは登録リストとも呼ばれ、図２２に示すように、その時点で信頼できる（秘密が露呈していない）装置のＩＤがリストアップされ、単調増加するバージョンナンバとともにセンタ（キー発行機関）のディジタル署名が施されたものである。

図１９において、記録再生装置は乱数Ｒ_Bを発生させ、キー発行機関に送る。

キー発行機関は、乱数Ｋ_A及びＲ_Aを発生させ、楕円曲線Ｅ上でシステム共通の点（ベースポイント）であるＧとＫ_Aを乗算してＶ_Aを計算し、さらに自分の秘密鍵（PriKey_A）を用いてデータＲ_A || Ｒ_B || Ｖ_Aに対して施した署名とともに、公開鍵証明書（Cert_A, Ｒ_A,Ｒ_B,Ｖ_A）を記録再生装置に送る。

記録再生装置は、キー発行機関の公開鍵証明書の正当性、キー発行機関が作成した署名の正当性を検査する。そして、自分がリボケーションリストを格納していれば、相手のＩＤがリボケーションリストに載っていないことを、また、自分がレジストレーションリストを格納していれば、相手のＩＤがレジストレーショ

ンリストに登録されていることを確認する。以上の確認が正常にできなければ、記録再生装置はキー発行機関が不正者と判断して処理を終了する。以上の確認が正常にできれば、記録再生装置は、乱数K_Bを生成して、キー発行機関が行ったのと同様な計算を行い、公開鍵証明書（Cert_B，R_B，R_A，V_B）とともにデータR_B || R_A || V_Bに対して施した署名をキー発行機関に送る。

キー発行機関では、上で記録再生装置が行ったのと同様の検査を受信したデータに対して行い、全ての検査が正常に終了したときのみ処理を継続する。

この後、キー発行機関ではK_AとV_Bを、記録再生装置ではK_BとV_Aを、それぞれ楕円曲線E上で乗算してセッションキーK_Sを得る。セッションキーの使用方法については、上述の図１８と同様である。

なお、楕円曲線上の乗算やディジタル署名の生成及び検査方法については、現在 IEEE P1363 で規格制定中であり、そのドラフトに詳細が記されている。

図１７に戻り、ステップＳ１７０６に進み、必要な世代のマスターキーを記録再生装置が入手できたか否かを検査する。入手できていれば、ステップＳ１７０３に進み、結局記録媒体へのデータの記録を行う。

必要な世代の暗号化マスターキーが取得できなければ、データの記録は行わずに処理を終了する。なお、この際に、必要な世代の暗号化マスターキーが取得できなかった旨のメッセージをユーザに対して表示してもよい。

なお、上記の例では、ステップＳ１７０５において、モデム１６０１を用い、電話回線を使用してキー発行機関からマスターキーを得るようにしているが、他の記録再生装置から得ることも可能であり、また、モデム５２ではなくディジタルＩ／Ｆ６２０を介したリンクからでもよい。キー発行機関からではなく、他の記録再生装置とマスターキーの授受を行う場合には、図１９に示した、公開鍵を用いた認証方式を用いることが好適である。

次に、図２３のフローチャートを参照して、記録媒体２００に記録されたデータの再生が行われる場合の、図１６に示す記録再生装置１６００の動作について説明する。

図２３において、ステップＳ２３０１乃至Ｓ２３０６の処理は、図１２のステップＳ１２０１乃至Ｓ１２０６の各処理と同様であるため、説明を省略する。但

し、ステップＳ２３０４においては、再生装置が格納する暗号化マスターキーの世代が、記録時世代情報に表される世代よりも古い場合には、ステップＳ２３０７に進む。

ステップＳ２３０７では、図１７のステップＳ１７０５と同様の方法を用いて、最新世代の暗号化マスターキーの取得を試みる。すなわち、記録再生装置１６００はモデム１６０１を使用してキー発行機関と電話回線を介してリンクを張り、キー発行機関が送信した最新世代の暗号化マスターキーを受信して取得する。なお、この際に、記録再生装置とキー発行機関は、上述の相互認証のプロトコルを実行することが好ましい。

次に、ステップＳ２３０８では、ステップＳ２３０７において必要な世代の暗号化マスターキーを取得できていればステップＳ２３０５に進み、結局記録媒体２００からデータの読み出しを行う。一方、必要な世代の暗号化マスターキーを取得できていなければ、データの読出しを行わずに処理を終了する。なお、この際に、必要な世代の暗号化マスターキーが取得できなかった旨のメッセージをユーザに対して表示してもよい。

なお、前述の図１３乃至図１５を用いて説明したＩＣカードを使用したマスターキー更新処理においても、記録再生装置１３００とＩＣカード１３０２間の機器間相互認証処理を実行して、認証が成立したことを条件として更新マスターキーの取得処理を実行する構成としてもよい。また、先に説明した図６の構成を持つ記録再生装置６００においても、例えばディジタルＩ／Ｆ６２０を介したネットワーク通信により、マスターキーを取得する際に、上述の認証処理を実行して、その認証が成立した場合にのみ、更新マスターキーの取得処理を実行する構成とすることが好ましい。

（３．３．キー更新端末を介するマスターキー更新構成）

次に、本発明の実施例として、情報記録又は再生装置と別体な独立した機器として構成されるキー更新端末を用いた構成例を説明する。具体的には、前述の図１０のＳ１００５において、最新マスターキーの取得を促すメッセージが表示された場合に、マスターキーの更新をするため、特殊なツール、即ち、キー更新端末を使用してマスターキー更新を行う構成である。キー更新端末は、例えばサー

ビスセンタから派遣されるサービスマンが保有する。本実施例は、このようなキー更新端末を用いた構成である。

前述したように、記録媒体を用いたキー更新構成においては、ひとつのカテゴリに複数、例えば数千台の装置が属する構成である。したがって、１つのカテゴリに含まれる多数の記録再生装置中の１台でも内部に安全に格納すべきデバイスキーが暴かれた場合、このカテゴリに含まれる全ての装置をシステムから排除しなくてはならない。本実施例のキー更新構成では、一旦、排除された装置のうち排除されるべきでない装置をシステム内に復活、即ちキー更新端末を利用してマスターキーの更新を行うことにより再び正常な記録再生を可能とした構成である。以下、キー更新端末を利用したマスターキー更新構成の複数の態様について説明する。

（３．３．１．キー更新端末を介するマスターキー更新構成例－１）

まず、前述の図６と同様の構成を持つ情報記録又は再生装置において、キー更新端末を介するマスターキーの更新処理を行う構成について説明する。但し、本実施例構成においては、情報記録又は再生装置は、装置の属するカテゴリ番号と、それに対応する鍵としてのデバイスキーに加えて、装置固有の識別番号としてのデバイスＩＤ（Ｄｅｖｉｃｅ　ＩＤ）と、デバイスＩＤに対応する装置固有鍵としてのデバイス固有キー（Ｄｅｖｉｃｅ　Ｕｎｉｑｕｅ　Ｋｅｙ）を安全に格納している。デバイス固有キーは、例えば先に説明した図１の暗号処理部内に格納される。

本実施例の構成では、情報記録又は再生装置のマスターキーを更新するため、キー更新用の情報処理装置（以下これをキー更新端末と呼ぶ）を用いる。キー更新端末の構成例を示すブロック図を図２４に示す。

図２４に示すように、キー更新端末２４００は、制御部２４０１、モデム２４０２、ディジタルインタフェース（Ｉ／Ｆ）２４０３を有する。図２４のキー更新端末２４００は、例えば、前述した通常の記録媒体を用いたキー更新において、その装置の属するカテゴリがリボークされ、カテゴリの識別により更新対象から排除され、その装置が新しいマスターキーを得られない場合に、個々の記録再生装置が、直接キー発行機関からマスターキーを得るための通信路を提供する。

図２５に、情報記録又は再生装置が図２４のキー更新端末を用いてキー発行機関からマスターキーを得るための通信路を確立する処理構成を示す。記録再生機装置２５００はディジタルＩ／Ｆ２５０１を有する。このディジタルＩ／Ｆ２５０１は、通常、音楽や映画などのコンテンツデータを伝送するのに用いられるが、キー発行機関からマスターキーを得る場合には、このディジタルＩ／Ｆ２５０１と、キー更新端末２４００のディジタルＩ／Ｆ２４０３を結び、キー更新端末２４００のモデム２４０２により電話回線を介してキー発行機関までの通信路を確立する。制御部２４０１は、通信制御、通信データのフォーマット変換処理制御、通信データの選択処理制御等を実行する。

キー更新端末２４００を介して、記録再生機装置２５００がキー発行機関との通信路を確立した後は、図２６に示す、共通鍵暗号技術を用いた相互認証及び鍵共有プロトコル、又は、図２７に示す、公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルを用いてキー発行機関と記録再生装置は互いの正当性を確認した後、キー発行機関が記録再生装置に最新のマスターキーを与える。

図２６、図２７は、先に説明した図１８の共通鍵暗号技術を用いた相互認証及び鍵共有プロトコル、図１９の公開鍵暗号技術を用いた相互認証及び鍵共有プロトコルと同様の処理シーケンスであるので、詳細な説明は図１８，１９を参照されたい。但し、図２６に示す共通鍵暗号技術を用いた相互認証及び鍵共有プロトコルにおいては、図１８の処理シーケンスにおいて秘密鍵として用いたデバイスキー（ＤＫ）に変えて、記録再生装置の各々に固有なキーであるデバイス固有キー（ＤＵＫ）を秘密鍵とした処理を実行する。したがって、キー発行機関は、個々の記録再生装置の機器ＩＤと対応するデバイス固有キーとのテーブルを持つ。

図２６又は図２７の相互認証、鍵共有プロトコルは、図２５で示すキー更新端末２４００を介して記録再生機装置２５００とキー発行機関との間で実行される。これらの処理の後の更新マスターキーの送信には、上記プロトコルにおいて共有したセッションキーＫ＿Ｓで更新マスターキーを暗号化して送信することで安全な更新マスターキーの伝送が可能である。

なお、キー発行機関から記録再生装置に対して、認証を行った後に更新マスターキーを伝送するのではなく、相互認証を省略して、記録再生装置の機器ＩＤ

（Ｄｅｖｉｃｅ　ＩＤ）のみを更新要求を行う記録再生装置から受信して、キー発行機関が有する、機器ＩＤとデバイス固有キーとのテーブルから、個々の記録再生装置のデバイス固有キー（ＤＵＫ：Ｄｅｖｉｃｅ　Ｕｎｉｑｕｅ　Ｋｅｙ）を取り出して、デバイス固有キー（ＤＵＫ）でマスターキーを暗号化して各記録再生装置に送信する構成としてもよい。暗号化されたマスターキーを受信した記録再生装置は、自身の有するデバイス固有キー（ＤＵＫ）で復号して更新マスターキーを取得する。この場合、記録再生装置が通信をする相手は、キー発行機関のように信頼が必要なものではなく、単に図２８のようなマスターキーテーブルを格納しているサーバなどでもよい。図２８のテーブルは、１つのカテゴリ内の個々の記録再生装置に対応付けて生成されたテーブルであり、記録再生装置の機器ＩＤである装置固有識別番号と、対応する記録再生装置のデバイス固有キー（ＤＵＫ）で暗号化された第ｎ世代のマスターキー（ＭＫ＿ｎ）が対応付けられて格納されたテーブルである。マスターキーの更新を実行する記録再生装置は、キー更新端末を介して図２８に示すテーブルを格納したサーバにアクセスして、自身のデバイス固有キー（ＤＵＫ）で暗号化された第ｎ世代のマスターキー（ＭＫ＿ｎ）を取得する。

（３．３．２．キー更新端末を介するマスターキー更新構成例－２）

次に、キー更新端末を介するマスターキー更新構成例の第２の実施例として、記録再生装置の通信インタフェース（Ｉ／Ｆ）にキー更新端末に接続して更新マスターキーを取得する構成例を説明する。

本実施例における記録再生装置は、図２９に示すように記録再生装置２９００の通信Ｉ／Ｆ２９０１を介してキー更新端末２９５０の通信Ｉ／Ｆ２９５１に接続し、前述の例と同様に制御部２９５１の制御のもとにモデム２９５２を介して鍵発行機関と接続して、前述の相互認証処理、鍵共有プロトコルを実行して、更新マスターキーを取得する。記録再生装置２９００の通信Ｉ／Ｆ２９０１は、赤外線通信やブルートゥース（Ｂｌｕｅｔｏｏｔｈ）などの無線通信方式とすることも可能である。

（３．３．３．キー更新端末を介するマスターキー更新構成例－３）

上述した２つの例では、鍵発行センタとの通信路をキー更新端末を介して確立

して通信により、更新マスターキーを取得していた。第３の例は、キー更新端末が、記録再生装置とキー発行機関の間の通信路を確立するのではなく、それ自体がキー発行機関もしくは上記のサーバとして働く。すなわち、キー更新端末中に、記憶手段を持っており、例えば図２８に示したマスターキーテーブルを記憶手段に格納した構成を持つ。

図３０及び図３１に本構成例の更新マスターキーの取得処理を説明する図を示す。図３０において、記録再生機装置３０００はディジタルＩ／Ｆ３００１を有する。このディジタルＩ／Ｆ３００１は、通常、音楽や映画などのコンテンツデータを伝送するのに用いられるが、キー更新端末３０５０からマスターキーを得る場合には、このディジタルＩ／Ｆ３００１と、キー更新端末３０５０のディジタルＩ／Ｆ３０５３を結び、キー更新端末３０５０の記録媒体３０５３に格納された、例えば図２８に示す暗号化マスターキー格納テーブルから、自身の機器ＩＤに対応する暗号化マスターキーを取得する。制御部３０５１は、記録再生機装置３０００とキー更新端末３０５０間の通信制御等を実行する。

また図３１に示すように記録再生装置３１００の通信Ｉ／Ｆ３１０１を介してキー更新端末３１５０の通信Ｉ／Ｆ３１５１に接続し、前述の例と同様にキー更新端末３１５０の記録媒体３１５３に格納された、例えば図２８に示す暗号化マスターキー格納テーブルから、自身の機器ＩＤに対応する暗号化マスターキーを制御部３１５１の制御のもとに取得する。記録再生装置３１００の通信Ｉ／Ｆ３１０１は、赤外線通信やブルートゥース（Ｂｌｕｅｔｏｏｔｈ）などの無線通信方式とすることも可能である。

また本例においても、キー更新端末と記録再生装置が相互認証及び鍵交換プロトコルを実行し、互いの正当性を確認した後に、上記プロトコルで共有した暗号鍵を用いてキー更新端末が記録再生装置に安全にマスターキーを伝送する構成としてもよい。この際の処理は、先に説明した図２６の共通鍵暗号技術に基づいた認証及び鍵交換プロトコル又は図２７の公開鍵暗号技術に基づいた認証及び鍵交換プロトコルを適用することが可能である。

図２６の共通鍵暗号技術に基づいた認証及び鍵交換プロトコルを用いる場合には、キー更新端末にデバイス固有キー（ＤＵＫ：　Ｄｅｖｉｃｅ　Ｕｎｉｑｕｅ

Ｋｅｙ）テーブルを持たせておき、さらにデバイス固有キー（ＤＵＫ）が露呈したことがわかっている記録再生装置の機器ＩＤ（Ｄｅｖｉｃｅ　ＩＤ）にはその旨のマークをつけておき、マスターキーを渡さないようにする。

また図２７の公開鍵暗号技術に基づいた認証及び鍵交換プロトコルを用いる場合には、キー更新端末にデバイス固有キー（ＤＵＫ：　Ｄｅｖｉｃｅ　Ｕｎｉｑｕｅ　Ｋｅｙ）テーブルは必要ないが、やはりデバイス固有キー（ＤＵＫ）が露呈したことがわかっている記録再生装置にマスターキーを渡さないために、それらの機器ＩＤ（Ｄｅｖｉｃｅ　ＩＤ）をリストにしたリボケーションリストをキー更新端末に格納しておき、キー更新要求のあった記録再生装置の機器ＩＤに対応する危機ＩＤがリストに載っていない装置にのみマスターキーを渡すようにする。

このように、キー更新端末を介するマスターキー更新構成を用いることにより、記録再生器とは別体として構成されるキー更新端末装置を介する更新キーの入手が可能となり、例えば、同一カテゴリに属する他の機器のデバイスキーの露呈によってマスターキーの更新が必要となった機器が、キー更新端末を介してキー発行機関と通信路を確立して、もしくは、キー更新端末から直接、マスターキーを入手することが可能となり、同一のカテゴリに属する端末中の個々の端末に対して個別の対応が可能となる。また、キー更新端末は、記録再生機器とは別に、更新処理を必要とする場合にのみ記録再生器に接続して使用する構成とすればよく、記録再生装置に通常備わるインタフェースを介して情報をやりとりできるため、記録再生装置にモデムなどを設けてコストアップさせる必要がない点でも優れている。

［４．キー配信構成としてのツリー（木）構造について］

次に、図６に示した記録再生装置が、データを記録媒体に記録、もしくは記録媒体から再生する際に必要なマスターキーを、ツリー構造の鍵配信構成を用いて各機器に配布する構成について説明する。図３２は、本方式を用いた記録システムにおける記録再生装置の鍵の配布構成を示した図である。図３２の最下段に示すナンバ０～１５が個々の記録再生装置である。すなわち図３２に示す木（ツリー）構造の各葉(リーフ：leaf)がそれぞれの記録再生装置に相当する。

各デバイス０～１５は、製造時（出荷時）に、予め定められている初期ツリーにおける、自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノードキー）及び各リーフのリーフキーを自身で格納する。図３２の最下段に示すＫ０００００～Ｋ１１１１が各デバイス０～１５にそれぞれ割り当てられたリーフキーであり、最上段のＫＲから、最下段から２番目の節（ノード）に記載されたキー：ＫＲ～Ｋ１１１をノードキーとする。

図３２に示すツリー構成において、例えばデバイス０はリーフキーＫ００００と、ノードキー：Ｋ０００、Ｋ００、Ｋ０、ＫＲを所有する。デバイス５はＫ０１０１、Ｋ０１０、Ｋ０１、Ｋ０、ＫＲを所有する。デバイス１５は、Ｋ１１１１、Ｋ１１１、Ｋ１１、Ｋ１、ＫＲを所有する。なお、図３２のツリーにはデバイスが０～１５の１６個のみ記載され、ツリー構造も４段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

また、図３２のツリー構造に含まれる各記録再生器には、様々な記録媒体、例えばＤＶＤ、ＣＤ、ＭＤ、メモリスティック（商標）等を使用する様々なタイプの記録再生器が含まれている。さらに、様々なアプリケーションサービスが共存することが想定される。このような異なるデバイス、異なるアプリケーションの共存構成の上に図３２に示すキー配布構成が適用されている。

これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図３２の点線で囲んだ部分、即ちデバイス０，１，２，３を同一の記録媒体を用いるひとつのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、共通に使用するマスターキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行う機関は、図３２の点線で囲んだ部分、即ちデバイス０，１，２，３を１つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図３２のツリー中に複数存在する。

なお、ノードキー、リーフキーは、ある１つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行うプロバイダ、決済機関等によってグループ毎に管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

このツリー構造において、図３２から明らかなように、１つのグループに含まれる３つのデバイス０，１，２，３はノードキーとして共通のキーＫ００、Ｋ０、ＫＲを保有する。このノードキー共有構成を利用することにより、例えば共通のマスターキーをデバイス０，１，２，３のみに提供することが可能となる。例えば、共通に保有するノードキーＫ００自体をマスターキーとして設定すれば、新たな鍵送付を実行することなくデバイス０，１，２，３のみが共通のマスターキーの設定が可能である。また、新たなマスターキーKmasterをノードキーＫ００で暗号化した値Ｅｎｃ（Ｋ００，Kmaster）を、ネットワークを介してあるいは記録媒体に格納してデバイス０，１，２，３に配布すれば、デバイス０，１，２，３のみが、それぞれのデバイスにおいて保有する共有ノードキーＫ００を用いて暗号Ｅｎｃ（Ｋ００，Kmaster）を解いてマスターキー：Kmasterを得ることが可能となる。なお、Ｅｎｃ（Ｋａ，Ｋｂ）はＫｂをＫａによって暗号化したデータであることを示す。

また、ある時点ｔにおいて、デバイス３の所有する鍵：Ｋ００１１,Ｋ００１，Ｋ００,Ｋ０,ＫＲが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス０，１，２，３のグループ）で送受信されるデータを守るために、デバイス３をシステムから切り離す必要がある。そのためには、ノードキー：Ｋ００１,Ｋ００,Ｋ０,ＫＲをそれぞれ新たな鍵Ｋ（ｔ）００１,Ｋ（ｔ）００,Ｋ（ｔ）０,Ｋ（ｔ）Ｒに更新し、デバイス０，１，２にその更新キーを伝える必要がある。ここで、Ｋ（ｔ）ａａａは、鍵Ｋａａａの世代（Generation）：ｔの更新キーであることを示す。

更新キーの配布処理について説明する。キーの更新は、例えば、図３３（Ａ）に示すキー更新ブロック（ＫＲＢ：Key Renewal Block）と呼ばれるブロックデータによって構成されるテーブルを例えばネットワーク、あるいは記録媒体に格納

してデバイス０，１，２に供給することによって実行される。

図３３（Ａ）に示すキー更新ブロック（ＫＲＢ）には、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図３３の例は、図３２に示すツリー構造中のデバイス０，１，２において、世代ｔの更新ノードキーを配布することを目的として形成されたブロックデータである。図３２から明らかなように、デバイス０，デバイス１は、更新ノードキーとしてＫ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要であり、デバイス２は、更新ノードキーとしてＫ（ｔ）００１、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要である。

図３３（Ａ）のＫＲＢに示されるようにＫＲＢには複数の暗号化キーが含まれる。最下段の暗号化キーは、Ｅｎｃ（Ｋ００１０，Ｋ（ｔ）００１）である。これはデバイス２の持つリーフキーＫ００１０によって暗号化された更新ノードキーＫ（ｔ）００１であり、デバイス２は、自身の持つリーフキーによってこの暗号化キーを復号し、Ｋ（ｔ）００１を得ることができる。また、復号により得たＫ（ｔ）００１を用いて、図３３（Ａ）の下から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００１，Ｋ（ｔ）００）を復号可能となり、更新ノードキーＫ（ｔ）００を得ることができる。以下順次、図３３（Ａ）の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図３３（Ａ）の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号しＫ（ｔ）Ｒを得る。一方、デバイス０，１は、ノードキーＫ０００は更新する対象に含まれておらず、更新ノードキーとして必要なのは、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒである。デバイス０，１は、図３３（Ａ）の上から３段目の暗号化キーＥｎｃ（Ｋ０００，Ｋ（ｔ）００）を復号しＫ（ｔ）００を取得し、以下、図３３（Ａ）の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図３３（Ａ）の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号しＫ（ｔ）Ｒを得る。このようにして、デバイス０，１，２は更新した鍵Ｋ（ｔ）００，Ｋ（ｔ）０，Ｋ（ｔ）Ｒを得ることができる。なお、図３３（Ａ）のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

図３２に示すツリー構造の上位段のノードキー：Ｋ０,ＫＲの更新が不要であり、ノードキーＫ００のみの更新処理が必要である場合には、図３３（Ｂ）のキー更新ブロック（ＫＲＢ：Key Renewal Block）を用いることで、更新ノードキーＫ（ｔ）００をデバイス０，１，２に配布することができる。

図３３（Ｂ）に示すＫＲＢは、例えば特定のグループにおいて共有する新たなマスターキーを配布する場合に利用可能である。具体例として、図３２に点線で示すグループ内のデバイス０，１，２，３がある記録媒体を用いており、新たな共通のマスターキーＫ（ｔ）masterが必要であるとする。このとき、デバイス０，１，２，３の共通のノードキーＫ００を更新したＫ（ｔ）００を用いて新たな共通の更新マスターキー：Ｋ（ｔ）masterを暗号化したデータＥｎｃ（Ｋ（ｔ），Ｋ（ｔ）master）を図３３（Ｂ）に示すＫＲＢとともに配布する。この配布により、デバイス４など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

すなわち、デバイス０，１，２はＫＲＢを処理して得たＫ（ｔ）００を用いて上記暗号文を復号すれば、ｔ時点でのマスターキーＫ（ｔ）masterを得ることが可能になる。

［ＫＲＢを使用したマスターキーの配布］

図３４に、ｔ時点でのマスターキーＫ（ｔ）masterを得る処理例として、Ｋ（ｔ）００を用いて新たな共通のマスターキーＫ（ｔ）masterを暗号化したデータＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）master）と図３３（Ｂ）に示すＫＲＢとを記録媒体を介して受領したデバイス０の処理を示す。

図３４に示すように、デバイス０は、記録媒体に格納されている世代：t時点のＫＲＢと自分が予め格納しているノードキーＫ０００を用いて上述したと同様のＫＲＢ処理により、ノードキーＫ（ｔ）００を生成する。さらに、復号した更新ノードキーＫ（ｔ）００を用いて更新マスターキーＫ（ｔ）masterを復号して、後にそれを使用するために自分だけが持つリーフキーＫ０００００で暗号化して格納する。なお、デバイス０が更新マスターキーＫ（ｔ）master を安全に自身内に格納できる場合、リーフキーＫ０００００で暗号化する必要はない。

また、この更新マスターキーの取得処理を図３５のフローチャートにより説明

する。なお、記録再生装置は出荷時にその時点で最新のマスターキー:K（c）masterを与えられ、自身のメモリに安全に（具体的には例えば、自身のリーフキーで暗号化して）格納しているものとする。

更新マスターキーK（n）masterとKRBの格納された記録媒体が、記録再生装置にセットされると、まず最初に、ステップS3501において、記録再生装置は、記録媒体から、記録媒体に格納されているマスターキーK（n）masterの時点（世代）番号：n（これを、プレ（pre－recording）記録世代情報（Generation#n）と呼ぶことにする）を読み出す。記録媒体には、予め、マスターキーK（n）masterの時点（世代）番号：nが記憶されている。また、自身が保持している暗号化マスターキーCを読み出し、ステップS3502において、その暗号化マスターキーの世代：cと、プレ記録世代情報Generation#nが表す世代：nとを比較して、その世代の前後を判定する。

ステップS3502において、プレ記録世代情報Generation#nが表す世代：nの方が、自身のメモリに記憶された暗号化マスターキーCの世代：cよりも後でない（新しくない）と判定された場合、即ち、メモリに記憶された暗号化マスターキーCの世代：cが、プレ記録世代情報Generation#nが表す世代：nと同一か、又は後の場合、ステップS3503乃至S3508をスキップして、マスターキー更新処理を終了する。すなわち、この場合、自身のメモリに記憶されたマスターキーK（c）master（暗号化マスターキーC）の更新は行う必要がないので、その更新は行われない。

一方、ステップS3502において、プレ記録世代情報Generation#nが表す世代：nの方が、メモリに記憶された暗号化マスターキーCの世代：cよりも後である（新しい）と判定された場合、即ち、メモリに記憶された暗号化マスターキーCの世代が、プレ記録世代情報Generation#nが表す世代nよりも前の世代である場合、ステップS3503に進み、記録再生装置は、記録媒体から、キー更新ブロック（KRB：Key Renewal Block）を読み出す。

ステップS3504において、記録再生装置は、ステップS3503で読み出したKRBと、自身がメモリに格納しているリーフキー（図32のデバイス0におけるK0000）及びノードキー（図32のデバイス0におけるK000,K0

０...）を用いて、プレ記録世代情報Generation#n（図３４におけるｔ）時点でのノード００の鍵Ｋ（ｔ）００を計算する。

ステップＳ３５０５では、ステップＳ３５０４においてＫ（ｔ）００を得られたか否かを検査する。得られなかった場合は、その時点においてその記録再生装置がツリー構成のグループからリボーク（排除）されていることを示すので、ステップＳ３５０６乃至Ｓ３５０８をスキップしてマスターキー更新処理を終了する。

Ｋ（ｔ）００を得られた場合、ステップＳ３５０６に進み、記録媒体からＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）master）、即ち、Ｋ（ｔ）００を用いてｔ時点でのマスターキーを暗号化した値を読み出す。そしてステップＳ３５０７において、この暗号文をＫ（ｔ）００を用いて復号してＫ（ｔ）masterを計算する。

ステップＳ３５０８では、自身のみが持つリーフキー（図３２のデバイス０におけるＫ００００）を用いてＫ（ｔ）masterを暗号化してメモリに格納する。以上で、マスターキーの更新処理が完了する。

ところで、マスターキーは、時点（世代）０から昇順に使用されていくが、新しい世代のマスターキーから、古い世代のマスターキーを計算によりシステム内の各機器が求められる構成とすることが望ましい。すなわち、記録再生装置は、一方向性関数ｆを保持しており、その一方向性関数ｆに、自身が持つマスターキーを、そのマスターキーの世代と、必要なマスターキーの世代との差に対応する回数だけ適用することにより、調べた世代のマスターキーを作成する。

具体的には、例えば、記録再生装置に記憶されているマスターキーＭＫの世代が世代ｉ＋１であり、あるデータの再生に必要な（記録時に使用された）マスターキーＭＫの世代が世代ｉ－１である場合、マスターキーＫ（ｉ－１）masterは、記録再生装置において、一方向性関数ｆが２回用いられ、ｆ（ｆ（Ｋ（ｉ＋１）master））を計算することにより生成される。

また、記録再生装置に記憶されているマスターキーの世代が世代ｉ＋１であり、必要なマスターキーの世代が世代ｉ－２である場合、マスターキーＫ（ｉ－２）masterは、一方向性関数ｆを３回用いて、ｆ（ｆ（ｆ（Ｋ（ｉ＋１）master））））を計算することにより生成される。

ここで、一方向性関数としては、例えば、ハッシュ(hash)関数を用いることができる。具体的には、例えば、ＭＤ５(Message Digest 5)や、ＳＨＡ－１(Secure Hash Algorithm - 1)等を採用することができる。キーを発行するキー発行機関は、これらの一方向性関数を用いて自身の世代より前の世代を生成可能なマスターキーＫ（０）master，Ｋ（１）master，Ｋ（２）master・・・，Ｋ（Ｎ）masterを、予め求めておく。すなわち、まず最初に、第Ｎ世代のマスターキーＫ（Ｎ）masterを設定し、そのマスターキーＫ（Ｎ）masterに、一方向性関数を１回ずつ適用しいくことで、それより前の世代のマスターキーＫ（Ｎ－１）master，Ｋ（Ｎ－２）master，・・・，Ｋ（１）master，Ｋ（０）masterを順次生成しておく。そして、世代の小さい（前の）マスターキーＫ（０）masterから順番に使用していく。なお、自身の世代より前の世代のマスターキーを生成するのに用いる一方向性関数は、全ての記録再生装置に設定されているものとする。

また、一方向性関数としては、例えば、公開鍵暗号技術を採用することも可能である。この場合、キー発行機関は、公開鍵暗号方式の秘密鍵を所有し、その秘密鍵に対する公開鍵を、全ての再生装置に与えておく。そして、キー発行機関は、第０世代のマスターキーＫ（０）masterを設定し、そのマスターキーＫ（０）masterから使用していく。すなわち、キー発行機関は、第１世代以降のマスターキーＫ（ｉ）masterが必要になったら、その１世代前のマスターキーＫ（ｉ－１）masterを、秘密鍵で変換することにより生成して使用する。この場合、キー発行機関は、一方向性関数を用いて、Ｎ世代のマスターキーを、予め生成しておく必要がない。また、この方法によれば、理論上は、無制限の世代のマスターキーを生成することができる。なお、記録再生装置では、ある世代のマスターキーを有していれば、そのマスターキーを、公開鍵で変換することにより、その世代より前の世代のマスターキーを得ることができる。

［５．記録再生装置による記録媒体へのキー更新ブロック（ＫＲＢ）格納処理］

ところで、上述した例では、キー更新ブロック：ＫＲＢ (Key Renewal Block)が記録媒体に予め格納されている例を示したが、記録再生装置が入出力Ｉ／Ｆや、ＩＣカード、モデム等を介して他の機器から受信したＫＲＢ (Key Renewal Bloc

k）を、最初に記録媒体にデータを記録する際や、記録媒体にデータを記録するたび毎に記録媒体に記録するようにすることもできる。

すなわち、図３６に示すように、記録再生装置は予め、入出力Ｉ／Ｆや、ＩＣカード、モデム等を介してキー更新ブロック：ＫＲＢ（Key Renewal Block）とマスターキーをノードキーで暗号化した暗号文を入手し、自身の記憶手段に格納しておき、コンテンツデータの記録媒体に対する記録の際に、図３７に示すフローチャートに従って処理をする構成としてもよい。

図３７の処理フローについて説明する。ステップＳ３７０１において、データを記録しようとする記録媒体には既にキー更新ブロック：ＫＲＢ（Key Renewal Block）が記録されているか否かを検査する。既に記録媒体にキー更新ブロック：ＫＲＢ（Key Renewal Block）が記録されていた場合にはステップＳ３７０２をスキップして終了する（データの記録処理に進む）が、記録されていない場合には、ステップＳ３７０２に進み、図３８に示すように、自身の記憶手段に格納しているキー更新ブロック：ＫＲＢ（Key Renewal Block）とマスターキーを暗号化した暗号文を記録媒体に記録する処理を実行する。その処理の実行の後に、コンテンツデータの記録処理に進む。

本実施例における記録媒体の構成例を図３９に示す。図３９に示す記録媒体には、記録媒体世代番号が格納される。この記録媒体３９００には、この記録媒体３９００に対するデータの記録及び再生に必要なマスターキーＭＫの最小の世代を表す世代情報としての世代番号（Generation#n）が記録されている。ここで、この世代番号（Generation#n）は、例えば、記録媒体３９００の製造時に、予め記録されるものであり、前術のプレ記録世代情報（Pre Recording Generation#n）と同様である。

この図３９に示す記録媒体３９００に対するデータの記録及び再生に必要なマスターキーＭＫの最小の世代は世代番号：ｎである。世代番号：ｎは例えばシーケンシャルな世代番号として付与される。記録再生装置が自身の記憶手段に格納しているマスターキーの世代がｎより以前である場合は、図３９に示す記録媒体３９００に対する記録、及び記録媒体３９００からの再生が拒否される。

世代番号（プレ記録世代番号）が記録された記録媒体３９００を記録再生装置

に装着して記録あるいは再生を実行する場合には、世代番号（プレ記録世代番号）と各記録再生装置に格納されたマスターキーの世代番号の比較処理が記録再生装置において実行され、記録再生装置が自身の記憶手段の格納マスターキーの世代が記録媒体の世代番号（プレ記録世代番号）ｎより古いものである場合は、図３９に示す記録媒体３９００に対する記録、及び記録媒体３９００からの再生が行えない。

図３９に示す記録媒体３９００に対するデータの記録及び再生に必要なマスターキーＭＫの最小の世代はｎである。記録再生装置が自身の記憶手段に格納しているマスターキーの世代がｎと同一か、より新しい記録再生装置は、記録媒体３９００への記録が行える。しかし、記録再生装置が自身の記憶手段に格納しているマスターキーの世代がｎより古い場合には、記録媒体３９００へのデータの記録は許されず、たとえ不正装置が古いマスターキーを用いて記録を行ったとしても、正しい再生装置はこのデータを再生しない。また、記録媒体３９００に正当に記録されるデータは必ずｎと同一かより新しい世代のマスターキーに基づいて暗号化されて記録されるため、記録再生装置３９００が自身の記憶手段に格納しているマスターキーの世代がｎより古い場合には、この記録再生装置は記録媒体のデータを復号できない（再生できない）ことになる。

なお、プレ記録世代情報Generation#nは、記録媒体３９００において、その書き換えが不可能な領域（書き換え不可の領域）としての、例えば、リードインエリアに記録されており、これにより、キーテーブル及びプレ記録世代情報Generation#nが不正に書き換えられることを防止するようになっている。

図３９に示す記録媒体３９００に対するデータの記録は、その記録媒体３９００におけるプレ記録世代情報が表す世代以後の世代のマスターキーＭＫを有していなければ行うことができない（許可されない）ように、装置の設計を行う。したがって、ある世代ｎを表すプレ記録世代情報Generation#nが記録された記録媒体３９００が流通することで、記録媒体３９００に対する記録を行う記録装置や、その記録再生が可能な図６の記録再生装置におけるマスターキーの更新が促進され、これにより、前の世代のマスターキーＭＫを用いている記録装置や記録再生装置が減少していき、その結果、不正なデータの復号が防止される。

すなわち、プレ記録世代情報が記録されていない、例えば前述の図４を用いて説明した記録媒体（光ディスク）１５０に対しては、上述のように、マスターキーを更新していない記録装置によって、データの記録が可能であり、そのようにしてデータが記録された光ディスク１５０は、マスターキーを更新していない情報再生装置で再生することができてしまうが、一方、プレ記録世代情報が記録されている図３９を用いて説明した記録媒体３９００に対しては、プレ記録世代情報が表す世代以後の世代のマスターキーＭＫを有していなければ、データの記録が許可されない。すなわち、記録媒体３９００へのデータの記録を行うには、そこに記録されているプレ記録世代情報が表す世代以後の世代のマスターキーＭＫが必要となるから、マスターキーを更新していない記録装置によるデータの記録が防止される。

なお、マスターキーの更新処理は、入出力Ｉ／Ｆや、ＩＣカード、モデム等を介してキー更新ブロック：ＫＲＢ（Key Renewal Block）と更新マスターキーをノードキーで暗号化した暗号文を入手し、ＫＲＢ（Key Renewal Block）の処理により更新されたマスターキーを取得することができる。ＫＲＢ（Key Renewal Block）の処理可能なデバイスは、前述のようにＫＲＢ復号処理可能なノードキー、リーフキーを有するデバイスに限られるので、ＫＲＢ（Key Renewal Block）配信時に相互認証を行う必要がなく、正当なデバイスのみが更新されたマスターキーを取得可能となる。

［６．データ処理手段の構成］

なお、上述した一連の処理は、ハードウェアにより行うことは勿論、ソフトウェアにより行うこともできる。すなわち、例えば、暗号処理手段６５０は暗号化／復号ＬＳＩとして構成することも可能であるが、汎用のコンピュータや、１チップのマイクロコンピュータにプログラムを実行させることにより行う構成とすることも可能である。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、汎用のコンピュータや１チップのマイクロコンピュータ等にインストールされる。図４０は、上述した一連の処理を実行するプログラムがインストールされるコンピュータの一実施の形態の構成例を示している。

プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク４００５やＲＯＭ４００３に予め記録しておくことができる。あるいは、プログラムはフロッピーディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体４０１０に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体４０１０は、いわゆるパッケージソフトウェアとして提供することができる。

なお、プログラムは、上述したようなリムーバブル記録媒体４０１０からコンピュータにインストールする他、ダウンロードサイトから、ディジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、ＬＡＮ(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通信部４００８で受信し、内蔵するハードディスク４００５にインストールすることができる。

コンピュータは、ＣＰＵ(Central Processing Unit)４００２を内蔵している。ＣＰＵ４００２には、バス４００１を介して、入出力インタフェース４０１１が接続されており、ＣＰＵ４００２は、入出力インタフェース４０１０を介して、ユーザによって、キーボードやマウス等で構成される入力部４００７が操作されることにより指令が入力されると、それに従って、ＲＯＭ(Read Only Memory)４００３に格納されているプログラムを実行する。

あるいは、ＣＰＵ４００２は、ハードディスク４００５に格納されているプログラム、衛星もしくはネットワークから転送され、通信部４００８で受信されてハードディスク４００５にインストールされたプログラム、又はドライブ４００９に装着されたリムーバブル記録媒体４０１０から読み出されてハードディスク４００５にインストールされたプログラムを、ＲＡＭ(Random Access Memory)４００４にロードして実行する。

これにより、ＣＰＵ４００２は、上述したフローチャートに従った処理、あるいは上述したブロック図の構成により行われる処理を行う。そして、ＣＰＵ４００２は、その処理結果を、必要に応じて、例えば、入出力インタフェース４０１

１を介して、ＬＣＤ(Liquid Crystal Display)やスピーカ等で構成される出力部４００６から出力、あるいは、通信部４００８から送信、さらには、ハードディスク４００５に記録させる。

ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。

また、プログラムは、１つのコンピュータにより処理されるものであってもよいし、複数のコンピュータによって分散処理されるものであってもよい。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであってもよい。

なお、本実施の形態では、コンテンツの暗号化／復号を行うブロックを、１チップの暗号化／復号ＬＳＩで構成する例を中心として説明したが、コンテンツの暗号化／復号を行うブロックは、ＣＰＵが実行する１つのソフトウェアモジュールとして実現することも可能である。

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用をなしうることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、特許請求の範囲の欄を参酌すべきである。

産業上の利用可能性

本発明の情報記録再生装置及び方法によれば、記録あるいは再生時に必要な世代の第１のキーを装置が有していない場合に、ユーザに対してキーの更新を促すメッセージを表示することでシステム全体のキーの更新を促進し、不正にデータが複製されることを防止することが可能となる。

加えて、本発明の情報記録再生装置及び方法によれば、記録あるいは再生時に必要な世代の第１のキーを装置が有していない場合に、外部の装置から必要な世代のキーを取得することにより、システム全体のキーの更新を促進し、不正にデ

ータが複製されることを防止することが可能となる。

さらに、本発明の情報記録再生装置及び方法によれば、暗号処理手段において、装置が格納する世代のキーに基づいて前の世代のキーを生成可能であり、インタオペラビリティを保ったまま、効果的に不正にデータが複製されることを防止することが可能となる。

さらに、本発明の情報記録媒体によれば、暗号化又は復号処理として使用可能なキーの世代を表す世代情報が記録されており、情報記録再生装置は、自身の格納するキーの世代と記録媒体に格納された世代情報との比較処理により、記録再生の可否が決定される。したがって、例えば無効となった過去のキーによる不正データの複製を防止することが可能となる。

さらに、本発明のキー更新端末装置及びキー更新方法によれば、記録再生器とは別体として構成されるキー更新端末装置を介する更新キーの入手が可能となり、例えば、同一カテゴリに属する他の機器のデバイスキーの露呈によってマスターキーの更新が必要となった機器が、キー更新端末を介してキー発行機関と通信路を確立、もしくは、キー更新端末から直接、マスターキーを入手することが可能となり、同一のカテゴリに属する端末中の個々の端末に対して個別の対応が可能となる。

さらに、本発明の情報記録再生装置及び方法によれば、ツリー（木）構造の鍵配布構成により、マスターキーの更新データを更新ブロック（ＫＲＢ）とともに送信する構成としたので、鍵更新の必要なデバイスにのみ復号可能な構成とした伝送又は配布が可能となり、メッセージ量を小さく抑えることができる。さらに、ツリー構造によって規定される特定のグループにのみ復号可能な鍵を配布可能であり、グループに属さない他のデバイスには復号できない構成とすることが可能であり、キー配信又は配布の安全性が確保される。

請求の範囲

1． 記録媒体に情報を記録する情報記録装置において、

世代毎に更新され、異なるキーとして設定される世代管理暗号化キーに基づく暗号処理によって前記記録媒体に対する格納情報の暗号処理を実行する暗号処理手段と、

前記情報記録装置の記憶手段に格納された装置格納世代管理暗号化キーの世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報とを比較し、前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、警告出力を実行するユーザインタフェースと、

を有することを特徴とする情報記録装置。

2． 前記装置格納世代管理暗号化キーは、複数の情報記録装置に共通に格納されたマスターキーであることを特徴とする請求の範囲第1項に記載の情報記録装置。

3． 前記暗号処理手段は、

前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、前記プレ世代情報の示す世代と同世代以降の世代管理暗号化キーに更新処理を実行する更新手段を含むことを特徴とする請求の範囲第1項に記載の情報記録装置。

4． 前記暗号処理手段は、

前記装置格納世代管理暗号化キーの世代情報よりも古い世代情報の世代管理暗号化キーを、前記装置格納世代管理暗号化キーに基づいて生成するキー生成手段を有する構成であることを特徴とする請求の範囲第1項に記載の情報記録装置。

5． 前記暗号処理手段は、

前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、前記プレ世代情報の示す世代と同世代以降の世代管理暗号化キーに更新処理を実行する更新手段を含み、

前記更新手段は、

暗号化処理の施された更新用世代管理暗号化キーについての復号処理を、前記情報記録装置に格納されたデバイスキーに基づいて実行し、更新された世代管理暗号化キーを生成する構成を有することを特徴とする請求の範囲第１項に記載の情報記録装置。

６．　前記暗号処理手段は、

前記暗号化処理の施された更新用世代管理暗号化キーと、復号用のデバイスキー識別子とを対応付けたキーテーブルを取得して、該キーテーブル中のデバイスキー識別子に基づいて識別されるデバイスキーにより、前記暗号化処理の施された更新用世代管理暗号化キーについての復号処理を実行する構成であることを特徴とする請求の範囲第５項に記載の情報記録装置。

７．　前記デバイスキーは、情報記録装置をカテゴリ区分し、共通のカテゴリに属する情報記録装置に共通のキーとした構成であることを特徴とする請求の範囲第５項に記載の情報記録装置。

８．　前記デバイスキーは、情報記録装置に付与されたシリアルナンバの区分に基づいて共通のキーとした構成であることを特徴とする請求の範囲第５項に記載の情報記録装置。

９．　前記情報記録装置は、

複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、

前記世代管理暗号化キーは、前記ノードキー又はリーフキーの少なくともいずれかを用いて更新可能なキーとして構成されていることを特徴とする請求の範囲第１項に記載の情報記録装置。

１０．　前記世代管理暗号化キーは、複数の情報記録装置において共通なマスターキーであることを特徴とする請求の範囲第９項に記載の情報記録装置。

１１．　前記ノードキーは、更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報記録装置に配布する構成であり、

前記情報記録装置における前記暗号処理手段は、

前記更新ノードキーで暗号化処理した前記世代管理暗号化キーの更新データを受領し、

キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記世代管理暗号化キーの更新データを取得する構成を有することを特徴とする請求の範囲第９項に記載の情報記録装置。

１２．　前記キー更新ブロック（ＫＲＢ）は、記録媒体に格納され、

前記暗号処理手段は、

前記記録媒体から読み出されたキー更新ブロック（ＫＲＢ）についての暗号処理を実行する構成であることを特徴とする請求の範囲第９項に記載の情報記録装置。

１３．　前記世代管理暗号化キーは、更新情報としての世代番号が対応付けられた構成であり、

前記暗号処理部は、

前記記録媒体に対する暗号化データ格納時に、使用した前記世代管理暗号化キーの世代番号を記録時世代番号として前記記録媒体に格納する構成を有することを特徴とする請求の範囲第９項に記載の情報記録装置。

１４．　記録媒体に情報を記録する情報記録装置において、

世代毎に更新され、異なるキーとして設定される世代管理暗号化キーに基づく暗号処理によって前記記録媒体に対する格納情報の暗号処理を実行する暗号処理手段と、

前記情報記録装置の記憶手段に格納された装置格納世代管理暗号化キーの世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報とを比較し、前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、前記プレ世代情報の示す世代又は該世代以降の世代管理暗号化キーの取得を実行するキー取得手段と、

を有することを特徴とする情報記録装置。

１５．　前記キー取得手段は、

ネットワークを介するデータ受信の実行可能な通信インタフェースを含むこと

を特徴とする請求の範囲第１４項に記載の情報記録装置。

１６．　前記キー取得手段は、

電話回線を介するデータ受信の実行可能な通信モデムを含むことを特徴とする請求の範囲第１４項に記載の情報記録装置。

１７．　前記キー取得手段は、

ＩＣカードを介するデータ受信の実行可能なＩ／Ｃカードインタフェースを含むことを特徴とする請求の範囲第１４項に記載の情報記録装置。

１８．　前記暗号処理手段は、

前記キー取得手段によるキー取得実行の際に、キー提供手段との相互認証処理を実行する構成を有し、

前記キー取得手段は、前記相互認証処理の成立を条件として前記世代管理暗号化キーの取得を実行する構成であることを特徴とする請求の範囲第１４項に記載の情報記録装置。

１９．　前記装置格納世代管理暗号化キーは、複数の情報記録装置に共通に格納されたマスターキーであることを特徴とする請求の範囲第１４項に記載の情報記録装置。

２０．　前記暗号処理手段は、

前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、前記プレ世代情報の示す世代と同世代以降の世代管理暗号化キーに更新処理を実行する更新手段を含むことを特徴とする請求の範囲第１４項に記載の情報記録装置。

２１．　前記暗号処理手段は、

前記装置格納世代管理暗号化キーの世代情報よりも古い世代情報の世代管理暗号化キーを、前記装置格納世代管理暗号化キーに基づいて生成するキー生成手段を有する構成であることを特徴とする請求の範囲第１４項に記載の情報記録装置。

２２．　前記暗号処理手段は、

前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、前記プレ世代情報の示す世代と同世代以降の世代管理暗号化キーに更新処理を実行する更新手段を含み、

前記更新手段は、

暗号化処理の施された更新用世代管理暗号化キーについての復号処理を、前記情報記録装置に格納されたデバイスキーに基づいて実行し、更新された世代管理暗号化キーを生成する構成を有することを特徴とする請求の範囲第１４項に記載の情報記録装置。

２３．　前記暗号処理手段は、

前記暗号化処理の施された更新用世代管理暗号化キーと、復号用のデバイスキー識別子とを対応付けたキーテーブルを取得して、該キーテーブル中のデバイスキー識別子に基づいて識別されるデバイスキーにより、前記暗号化処理の施された更新用世代管理暗号化キーについての復号処理を実行する構成であることを特徴とする請求の範囲第２２項に記載の情報記録装置。

２４．　前記デバイスキーは、情報記録装置をカテゴリ区分し、共通のカテゴリに属する情報記録装置に共通のキーとした構成であることを特徴とする請求の範囲第２２項に記載の情報記録装置。

２５．　前記デバイスキーは、情報記録装置に付与されたシリアルナンバの区分に基づいて共通のキーとした構成であることを特徴とする請求の範囲第２２項に記載の情報記録装置。

２６．　前記情報記録装置は、

複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、

前記世代管理暗号化キーは、前記ノードキー又はリーフキーの少なくともいずれかを用いて更新可能なキーとして構成されていることを特徴とする請求の範囲第１４項に記載の情報記録装置。

２７．　前記世代管理暗号化キーは、複数の情報記録装置において共通なマスターキーであることを特徴とする請求の範囲第２６項に記載の情報記録装置。

２８．　前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報記録装置に配布する構成であり、

前記情報記録装置における前記暗号処理手段は、

前記更新ノードキーで暗号化処理した前記世代管理暗号化キーの更新データを受領し、

キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記世代管理暗号化キーの更新データを取得する構成を有することを特徴とする請求の範囲第２６項に記載の情報記録装置。

２９．　前記キー更新ブロック（ＫＲＢ）は、記録媒体に格納され、

前記暗号処理手段は、

前記記録媒体から読み出されたキー更新ブロック（ＫＲＢ）についての暗号処理を実行する構成であることを特徴とする請求の範囲第２６項に記載の情報記録装置。

３０．　前記世代管理暗号化キーは、更新情報としての世代番号が対応付けられた構成であり、

前記暗号処理部は、

前記記録媒体に対する暗号化データ格納時に、使用した前記世代管理暗号化キーの世代番号を記録時世代番号として前記記録媒体に格納する構成を有することを特徴とする請求の範囲第２６項に記載の情報記録装置。

３１．　記録媒体に情報を記録する情報記録装置において、

世代毎に更新され、異なるキーとして設定される世代管理暗号化キーに基づく暗号処理によって前記記録媒体に対する格納情報の暗号処理を実行する暗号処理手段と、

前記情報記録装置の記憶手段に格納された装置格納世代管理暗号化キーの世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報とを比較し、前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、前記プレ世代情報の示す世代又は該世代以降の世代管理暗号化キーを取得するためのキー更新端末を接続するキー更新端末接続インタフェースと、

を有することを特徴とする情報記録装置。

３２．　前記情報記録装置は、

前記キー更新端末からの前記世代管理暗号化キー取得実行の際に、前記キー更新端末との相互認証処理を実行する構成を有し、

前記情報記録装置は、前記相互認証処理の成立を条件として前記世代管理暗号化キーの取得を実行する構成であることを特徴とする請求の範囲第３１項に記載の情報記録装置。

３３．　前記情報記録装置は、

複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーとを保有し、

前記世代管理暗号化キーは、前記ノードキー又はリーフキーの少なくともいずれかを用いて更新可能なキーとして構成されていることを特徴とする請求の範囲第３１項に記載の情報記録装置。

３４．　前記世代管理暗号化キーは、複数の情報記録装置において共通なマスターキーであることを特徴とする請求の範囲第３３項に記載の情報記録装置。

３５．　前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報記録装置に配布する構成であり、

前記情報記録装置における前記暗号処理手段は、

前記更新ノードキーで暗号化処理した前記世代管理暗号化キーの更新データを受領し、

キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記世代管理暗号化キーの更新データを取得する構成を有することを特徴とする請求の範囲第３３項に記載の情報記録装置。

３６．　前記キー更新ブロック（ＫＲＢ）は、記録媒体に格納され、

前記暗号処理手段は、

前記記録媒体から読み出されたキー更新ブロック（ＫＲＢ）についての暗号処理を実行する構成であることを特徴とする請求の範囲第３３項に記載の情報記録

装置。

３７．　前記世代管理暗号化キーは、更新情報としての世代番号が対応付けられた構成であり、

前記暗号処理部は、

前記記録媒体に対する暗号化データ格納時に、使用した前記世代管理暗号化キーの世代番号を記録時世代番号として前記記録媒体に格納する構成を有することを特徴とする請求の範囲第３３項に記載の情報記録装置。

３８．　記録媒体から情報を再生する情報再生装置において、

世代毎に更新され、異なるキーとして設定される世代管理復号キーに基づく復号処理によって前記記録媒体から読み取られる情報の復号処理を実行する暗号処理手段と、

前記情報再生装置の記憶手段に格納された装置格納世代管理復号キーの世代情報と、前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報との比較において、前記記録時世代情報が前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に警告出力を実行するユーザインタフェースと、

を有することを特徴とする情報再生装置。

３９．　前記暗号処理手段は、

前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報との比較処理において前記プレ世代情報が前記記録時世代情報よりも新しいものである場合に復号処理を実行しない構成としたことを特徴とする請求の範囲第３８項に記載の情報再生装置。

４０．　前記装置格納世代管理復号キーは、複数の情報再生装置に共通に格納されたマスターキーであることを特徴とする請求の範囲第３８項に記載の情報再生装置。

４１．　前記暗号処理手段は、

前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、前記記録時世代情報の示す世代と同世代以降の世代管理復

号キーに更新処理を実行する更新手段を含むことを特徴とする請求の範囲第３８項に記載の情報再生装置。

４２．　前記暗号処理手段は、

前記装置格納世代管理復号キーの世代情報よりも古い世代情報の世代管理復号キーを、前記装置格納世代管理復号キーに基づいて生成するキー生成手段を有する構成であることを特徴とする請求の範囲第３８項に記載の情報再生装置。

４３．　前記暗号処理手段は、

前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、前記記録時世代情報の示す世代と同世代以降の世代管理復号キーに更新処理を実行する更新手段を含み、

前記更新手段は、

暗号化処理の施された更新用世代管理復号キーについての復号処理を、前記情報再生装置に格納されたデバイスキーに基づいて実行し、更新された世代管理復号キーを生成する構成を有することを特徴とする請求の範囲第３８項に記載の情報再生装置。

４４．　前記暗号処理手段は、

前記暗号化処理の施された更新用世代管理復号キーと、復号用のデバイスキー識別子とを対応付けたキーテーブルを取得して、該キーテーブル中のデバイスキー識別子に基づいて識別されるデバイスキーにより、前記暗号化処理の施された更新用世代管理復号キーについての復号処理を実行する構成であることを特徴とする請求の範囲第４３項に記載の情報再生装置。

４５．　前記デバイスキーは、情報再生装置をカテゴリ区分し、共通のカテゴリに属する情報再生装置に共通のキーとした構成であることを特徴とする請求の範囲第４３項に記載の情報再生装置。

４６．　前記デバイスキーは、情報再生装置に付与されたシリアルナンバの区分に基づいて共通のキーとした構成であることを特徴とする請求の範囲第４３項に記載の情報再生装置。

４７．　前記情報再生装置は、

複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノード

に固有のノードキーと各情報再生装置固有のリーフキーとを保有し、

前記世代管理復号キーは、前記ノードキー又はリーフキーの少なくともいずれかを用いて更新可能なキーとして構成されていることを特徴とする請求の範囲第３８項に記載の情報再生装置。

４８．　前記世代管理復号キーは、複数の情報再生装置において共通なマスターキーであることを特徴とする請求の範囲第４７項に記載の情報再生装置。

４９．　前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報再生装置に配布する構成であり、

前記情報再生装置における前記暗号処理手段は、

前記更新ノードキーで暗号化処理した前記世代管理復号キーの更新データを受領し、

キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記世代管理復号キーの更新データを取得する構成を有することを特徴とする請求の範囲第４７項に記載の情報再生装置。

５０．　前記キー更新ブロック（ＫＲＢ）は、記録媒体に格納され、

前記暗号処理手段は、

前記記録媒体から読み出されたキー更新ブロック（ＫＲＢ）についての暗号処理を実行する構成であることを特徴とする請求の範囲第４７項に記載の情報再生装置。

５１．　前記世代管理復号キーは、更新情報としての世代番号が対応付けられた構成であり、

前記暗号処理部は、

前記記録媒体からの暗号化データの復号時に、該暗号化データの暗号処理時に使用した世代管理暗号化キーの世代番号を前記記録媒体から読み取り、該読み取られた世代番号に対応する世代管理復号キーを使用して復号を実行する構成であることを特徴とする請求の範囲第４７項に記載の情報再生装置。

５２．　記録媒体から情報を再生する情報再生装置において、

世代毎に更新され、異なるキーとして設定される世代管理復号キーに基づく復号処理によって前記記録媒体から読み取られる情報の復号処理を実行する暗号処理手段と、

前記情報再生装置の記憶手段に格納された装置格納世代管理復号キーの世代情報と、前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報とを比較し、前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、前記記録時世代情報の示す世代又は該世代以降の世代管理復号キーの取得を実行するキー取得手段と、

を有することを特徴とする情報再生装置。

５３．　前記情報再生装置は、

前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報との比較処理を実行して該比較処理において前記プレ世代情報が前記記録時世代情報よりも新しいものである場合に再生処理を実行しない構成としたことを特徴とする請求の範囲第５２項に記載の情報再生装置。

５４．　前記キー取得手段は、

ネットワークを介するデータ受信の実行可能な通信インタフェースを含むことを特徴とする請求の範囲第５２項に記載の情報再生装置。

５５．　前記キー取得手段は、

電話回線を介するデータ受信の実行可能な通信モデムを含むことを特徴とする請求の範囲第５２項に記載の情報再生装置。

５６．　前記キー取得手段は、

ＩＣカードを介するデータ受信の実行可能なＩ／Ｃカードインタフェースを含むことを特徴とする請求の範囲第５２項に記載の情報再生装置。

５７．　前記暗号処理手段は、

前記キー取得手段によるキー取得実行の際に、キー提供手段との相互認証処理を実行する構成を有し、

前記キー取得手段は、前記相互認証処理の成立を条件として前記世代管理復号

キーの取得を実行する構成であることを特徴とする請求の範囲第５２項に記載の情報再生装置。

５８．　前記装置格納世代管理復号キーは、複数の情報再生装置に共通に格納されたマスターキーであることを特徴とする請求の範囲第５２項に記載の情報再生装置。

５９．　前記暗号処理手段は、

前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、前記記録時世代情報の示す世代と同世代以降の世代管理復号キーに更新処理を実行する更新手段を含むことを特徴とする請求の範囲第５２項に記載の情報再生装置。

６０．　前記暗号処理手段は、

前記装置格納世代管理復号キーの世代情報よりも古い世代情報の世代管理復号キーを、前記装置格納世代管理復号キーに基づいて生成するキー生成手段を有する構成であることを特徴とする請求の範囲第５２項に記載の情報再生装置。

６１．　前記暗号処理手段は、

前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、前記記録時世代情報の示す世代と同世代以降の世代管理復号キーに更新処理を実行する更新手段を含み、

前記更新手段は、

暗号化処理の施された更新用世代管理復号キーについての復号処理を、前記情報再生装置に格納されたデバイスキーに基づいて実行し、更新された世代管理復号キーを生成する構成を有することを特徴とする請求の範囲第５２項に記載の情報再生装置。

６２．　前記暗号処理手段は、

前記暗号化処理の施された更新用世代管理復号キーと、暗号復号用のデバイスキー識別子とを対応付けたキーテーブルを取得して、該キーテーブル中のデバイスキー識別子に基づいて識別されるデバイスキーにより、前記暗号化処理の施された更新用世代管理復号キーについての復号処理を実行する構成であることを特徴とする請求の範囲第６１項に記載の情報再生装置。

６３．　前記デバイスキーは、情報再生装置をカテゴリ区分し、共通のカテゴリに属する情報再生装置に共通のキーとした構成であることを特徴とする請求の範囲第６１項に記載の情報再生装置。

６４．　前記デバイスキーは、情報再生装置に付与されたシリアルナンバの区分に基づいて共通のキーとした構成であることを特徴とする請求の範囲第６１項に記載の情報再生装置。

６５．　前記情報再生装置は、

複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、

前記世代管理復号キーは、前記ノードキー又はリーフキーの少なくともいずれかを用いて更新可能なキーとして構成されていることを特徴とする請求の範囲第５２項に記載の情報再生装置。

６６．　前記世代管理復号キーは、複数の情報再生装置において共通なマスターキーであることを特徴とする請求の範囲第６５項に記載の情報再生装置。

６７．　前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報再生装置に配布する構成であり、

前記情報再生装置における前記暗号処理手段は、

前記更新ノードキーで暗号化処理した前記世代管理復号キーの更新データを受領し、

キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記世代管理復号キーの更新データを取得する構成を有することを特徴とする請求の範囲第６５項に記載の情報再生装置。

６８．　前記キー更新ブロック（ＫＲＢ）は、記録媒体に格納され、

前記暗号処理手段は、

前記記録媒体から読み出されたキー更新ブロック（ＫＲＢ）についての暗号処理を実行する構成であることを特徴とする請求の範囲第６５項に記載の情報再生

装置。

６９．　前記世代管理復号キーは、更新情報としての世代番号が対応付けられた構成であり、

前記暗号処理部は、

前記記録媒体からの暗号化データの復号時に、該暗号化データの暗号処理時に使用した世代管理暗号化キーの世代番号を前記記録媒体から読み取り、該読み取られた世代番号に対応する世代管理復号キーを使用して復号を実行する構成であることを特徴とする請求の範囲第６５項に記載の情報再生装置。

７０．　記録媒体から情報を再生する情報再生装置において、

世代毎に更新され、異なるキーとして設定される世代管理復号キーに基づく復号処理によって前記記録媒体から読み取られる情報の復号処理を実行する暗号処理手段と、

前記情報再生装置の記憶手段に格納された装置格納世代管理復号キーの世代情報と、前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報とを比較し、前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、前記記録時世代情報の示す世代又は該世代以降の世代管理復号キーを取得するためのキー更新端末を接続するキー更新端末接続インタフェースと、

を有することを特徴とする情報再生装置。

７１．　前記情報再生装置は、

前記キー更新端末からの前記世代管理復号キー取得実行の際に、前記キー更新端末との相互認証処理を実行する構成を有し、

前記情報再生装置は、前記相互認証処理の成立を条件として前記世代管理復号キーの取得を実行する構成であることを特徴とする請求の範囲第７０項に記載の情報再生装置。

７２．　前記情報再生装置は、

複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーとを保有し、

前記世代管理復号キーは、前記ノードキー又はリーフキーの少なくともいずれ

かを用いて更新可能なキーとして構成されていることを特徴とする請求の範囲第７０項に記載の情報再生装置。

７３．　前記世代管理復号キーは、複数の情報再生装置において共通なマスターキーであることを特徴とする請求の範囲第７２項に記載の情報再生装置。

７４．　前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報再生装置に配布する構成であり、

前記情報再生装置における前記暗号処理手段は、

前記更新ノードキーで暗号化処理した前記世代管理復号キーの更新データを受領し、

キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得するとともに、該取得した更新ノードキーに基づいて前記世代管理復号キーの更新データを取得する構成を有することを特徴とする請求の範囲第７２項に記載の情報再生装置。

７５．　前記キー更新ブロック（ＫＲＢ）は、記録媒体に格納され、

前記暗号処理手段は、

前記記録媒体から読み出されたキー更新ブロック（ＫＲＢ）についての暗号処理を実行する構成であることを特徴とする請求の範囲第７２項に記載の情報再生装置。

７６．　前記世代管理復号キーは、更新情報としての世代番号が対応付けられた構成であり、

前記暗号処理部は、

前記記録媒体からの暗号化データの復号時に、該暗号化データの暗号処理時に使用した世代管理暗号化キーの世代番号を前記記録媒体から読み取り、該読み取られた世代番号に対応する世代管理復号キーを使用して復号を実行する構成であることを特徴とする請求の範囲第７２項に記載の情報再生装置。

７７．　記録媒体に情報を記録する情報記録方法において、

世代毎に更新され、異なるキーとして設定される世代管理暗号化キーに基づく

暗号処理によって前記記録媒体に対する格納情報の暗号処理を実行する暗号処理ステップを有し、

さらに、

情報記録装置の記憶手段に格納された装置格納世代管理暗号化キーの世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報とを比較するステップと、

前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、警告出力を実行する警告出力ステップと、

を有することを特徴とする情報記録方法。

７８．　記録媒体に情報を記録する情報記録方法において、

世代毎に更新され、異なるキーとして設定される世代管理暗号化キーに基づく暗号処理によって前記記録媒体に対する格納情報の暗号処理を実行する暗号処理ステップを有し、

さらに、

情報記録装置の記憶手段に格納された装置格納世代管理暗号化キーの世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報とを比較するステップと、

前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、前記プレ世代情報の示す世代又は該世代以降の世代管理暗号化キーの取得を実行するキー取得ステップと、

を有することを特徴とする情報記録方法。

７９．　前記情報記録方法において、

前記キー取得ステップは、

複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーの少なくともいずれかを用いて前記世代管理暗号化キーの更新処理を実行する更新ステップと、

前記更新ステップにおいて更新された世代管理暗号化キーに基づいて前記記録媒体に格納するデータの暗号処理を実行する暗号処理ステップと、

を含むことを特徴とする請求の範囲第７８項に記載の情報記録方法。

８０．　前記世代管理暗号化キーは、複数の情報記録装置において共通なマスターキーであることを特徴とする請求の範囲第７９項に記載の情報記録方法。

８１．　前記情報記録方法において、

前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報記録装置に配布する構成であり、

前記更新ステップは、

前記キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得する更新ノードキー取得ステップと、

取得した更新ノードキーに基づいて前記世代管理暗号化キーの更新データを算出する更新データ取得ステップと、

を含むことを特徴とする請求の範囲第７９項に記載の情報記録方法。

８２．　前記世代管理暗号化キーは、更新情報としての世代番号が対応付けられた構成であり、

前記暗号処理ステップは、さらに、

前記記録媒体に対する暗号化データ格納時に、使用した前記世代管理暗号化キーの世代番号を記録時世代番号として前記記録媒体に格納するステップを含むことを特徴とする請求の範囲第７９項に記載の情報記録方法。

８３．　記録媒体から情報を再生する情報再生方法において、

世代毎に更新され、異なるキーとして設定される世代管理復号キーに基づく復号処理によって前記記録媒体の格納情報の復号処理を実行する復号処理ステップを有し、

さらに、

情報再生装置の記憶手段に格納された装置格納世代管理復号キーの世代情報と、前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報とを比較するステップと、

前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、警告出力を実行する警告出力ステップと、

を有することを特徴とする情報再生方法。

８４．　記録媒体から情報を再生する情報再生方法において、

世代毎に更新され、異なるキーとして設定される世代管理復号キーに基づく復号処理によって前記記録媒体の格納情報の復号処理を実行する復号処理ステップを有し、

さらに、

情報記録再生装置の記憶手段に格納された装置格納世代管理復号キーの世代情報と、前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報とを比較するステップと、

前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、前記記録時世代情報の示す世代又は該世代以降の世代管理復号キーの取得を実行するキー取得ステップと、

を有することを特徴とする情報再生方法。

８５．　前記情報再生方法において、

前記キー取得ステップは、

複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーの少なくともいずれかを用いて記録媒体に格納された暗号データの復号処理を実行する世代管理復号キーの更新処理を実行する更新ステップと、

前記更新ステップにおいて更新された世代管理復号キーに基づいて前記記録媒体に格納された暗号データの復号処理を実行する復号処理ステップと、

を含むことを特徴とする請求の範囲第８４項に記載の情報再生方法。

８６．　前記世代管理復号キーは、複数の情報再生装置において共通なマスターキーであることを特徴とする請求の範囲第８５項に記載の情報再生方法。

８７．　前記情報再生方法において、

前記ノードキーは更新可能なキーとして構成され、更新処理に際しては更新ノードキーを下位階層のノードキー又はリーフキーの少なくともいずれかを含むキーにより暗号化したキー更新ブロック（ＫＲＢ）を更新対象となるリーフの情報再生装置に配布する構成であり、

前記更新ステップは、

前記キー更新ブロック（ＫＲＢ）の暗号処理により、前記更新ノードキーを取得する更新ノードキー取得ステップと、

取得した更新ノードキーに基づいて前記世代管理復号キーの更新データを算出する更新データ取得ステップと、

を含むことを特徴とする請求の範囲第８５項に記載の情報再生方法。

８８．　前記世代管理復号キーは、更新情報としての世代番号が対応付けられた構成であり、

前記復号処理ステップは、

前記記録媒体からの暗号化データの復号時に、該暗号化データの暗号処理時に使用した世代管理暗号化キーの世代番号を前記記録媒体から読み取り、該読み取られた世代番号に対応する世代管理復号キーを使用して実行することを特徴とする請求の範囲第８５項に記載の情報再生方法。

８９．　情報の記録可能な情報記録媒体であって、

該情報記録媒体に対する暗号化データの書き込みに使用可能な暗号化キー、又は該情報記録媒体の格納データの復号処理に使用可能な復号キーとして許容されるキーの世代情報としてのプレ世代情報を格納したことを特徴とする情報記録媒体。

９０．　前記プレ世代情報は、前記情報記録媒体における書き換え不可領域に記録されていることを特徴とする請求の範囲第８９項に記載の情報記録媒体。

９１．　世代毎に更新され、異なるキーとして設定される世代管理キーに基づく処理によって記録媒体に対する格納情報の暗号化処理又は記録媒体から読み取られる情報の復号処理を実行する暗号処理手段を有する情報記録又は再生装置に対する更新世代管理キーの提供を行うキー更新端末装置であり、

前記情報記録又は再生装置に接続可能なインタフェースと、

外部との通信を実行する通信手段と、

前記インタフェースを介する前記情報記録又は再生装置からの装置固有識別子の取得処理、該装置固有識別子の前記通信手段を介する送信処理、前記通信手段を介する更新世代管理キーの受信処理、及び前記インタフェースを介する前記情

報記録又は再生装置に対する更新世代管理キーの転送処理の各制御を実行する制御手段と、

を有することを特徴とするキー更新端末装置。

９２．　世代毎に更新され、異なるキーとして設定される世代管理キーに基づく処理によって記録媒体に対する格納情報の暗号化処理又は記録媒体から読み取られる情報の復号処理を実行する暗号処理手段を有する情報記録又は再生装置に対する更新世代管理キーの提供を行うキー更新端末装置であり、

前記情報記録又は再生装置に接続可能なインタフェースと、

装置固有の暗号化鍵で暗号化された世代管理キーを、前記情報記録又は再生装置の装置固有識別子に対応付けたキーテーブルを格納した記憶手段と、

前記インタフェースを介する前記情報記録又は再生装置からの装置固有識別子の取得処理、該装置固有識別子に基づく前記記憶手段からの該装置固有識別子に対応する暗号化世代管理キーの取得処理、及び前記インタフェースを介する前記情報記録又は再生装置に対する更新世代管理キーの転送処理の各制御を実行する制御手段と、

を有することを特徴とするキー更新端末装置。

９３．　前記キー更新端末装置は、

前記情報記録又は再生装置との相互認証処理を実行する構成を有し、

前記キー更新端末装置は、前記相互認証処理の成立を条件として前記世代管理キーの前記情報記録又は再生装置に対する提供処理を実行する構成であることを特徴とする請求の範囲第９２項に記載のキー更新端末装置。

９４．　世代毎に更新され、異なるキーとして設定される世代管理キーに基づく処理によって記録媒体に対する格納情報の暗号化処理又は記録媒体から読み取られる情報の復号処理を実行する暗号処理手段を有する情報記録又は再生装置に対する更新世代管理キーの提供を行う世代管理キー更新方法であり、

前記情報記録又は再生装置に接続可能なインタフェースと、外部との通信を実行する通信手段とを有するキー更新端末装置を前記情報記録又は再生装置に接続するステップと、

前記インタフェースを介する前記情報記録又は再生装置からの装置固有識別子

の取得処理ステップと、

装置固有識別子の前記通信手段を介する送信処理ステップと、

前記通信手段を介する更新世代管理キーの受信処理ステップと、

前記インタフェースを介する前記情報記録又は再生装置に対する更新世代管理キーの転送処理ステップと、

を有することを特徴とする世代管理キー更新方法。

９５．　世代毎に更新され、異なるキーとして設定される世代管理キーに基づく処理によって記録媒体に対する格納情報の暗号化処理又は記録媒体から読み取られる情報の復号処理を実行する暗号処理手段を有する情報記録又は再生装置に対する更新世代管理キーの提供を行う世代管理キー更新方法であり、

前記情報記録又は再生装置に接続可能なインタフェースと、装置固有の暗号化鍵で暗号化された世代管理キーを、前記情報記録又は再生装置の装置固有識別子に対応付けたキーテーブルを格納した記憶手段とを有するキー更新端末装置を前記情報記録又は再生装置に接続するステップと、

前記インタフェースを介する前記情報記録又は再生装置からの装置固有識別子の取得処理ステップと、

装置固有識別子に基づく前記記憶手段からの該装置固有識別子に対応する暗号化世代管理キーの取得処理ステップと、

前記インタフェースを介する前記情報記録又は再生装置に対する更新世代管理キーの転送処理ステップと、

を有することを特徴とする世代管理キー更新方法。

９６．　前記世代管理キー更新方法において、さらに、

前記情報記録又は再生装置との相互認証処理を実行するステップを有し、

前記相互認証処理の成立を条件として前記世代管理キーの前記情報記録又は再生装置に対する提供処理を実行することを特徴とする請求の範囲第９５項に記載の世代管理キー更新方法。

９７．　記録媒体に情報を記録する情報記録処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

情報記録装置の記憶手段に格納された装置格納世代管理暗号化キーの世代情報と、前記記録媒体に予め格納された記録媒体世代情報であるプレ世代情報とを比較するステップと、

世代毎に更新され、異なるキーとして設定される世代管理暗号化キーに基づく暗号処理によって前記記録媒体に対する格納情報の暗号処理を実行する暗号処理ステップを有し、

さらに、

前記プレ世代情報が、前記装置格納世代管理暗号化キーの世代情報よりも新しいものである場合に、

警告出力ステップ、

あるいは前記プレ世代情報の示す世代又は該世代以降の世代管理暗号化キーの取得を実行するキー取得ステップと、

の少なくともいずれかを実行するステップ

を有することを特徴とするプログラム提供媒体。

９８．　前記コンピュータ・プログラムは、さらに、

複数の異なる情報記録装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報記録装置固有のリーフキーの少なくともいずれかを用いて記録媒体に対する格納データの暗号化処理を実行する世代管理暗号化キーの更新処理を実行する更新ステップを含むことを特徴とする請求の範囲第９７項に記載のプログラム提供媒体。

９９．　記録媒体から情報を再生する情報再生処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

情報再生装置の記憶手段に格納された装置格納世代管理復号キーの世代情報と、前記記録媒体に情報が記録された際に用いられた世代情報である記録時世代情報とを比較するステップと、

世代毎に更新され、異なるキーとして設定される世代管理復号キーに基づく復号処理によって前記記録媒体からの格納情報の復号処理を実行する復号処理ステップを有し、

さらに、

前記記録時世代情報が、前記装置格納世代管理復号キーの世代情報よりも新しいものである場合に、

警告出力ステップ、

あるいは前記記録時世代情報の示す世代又は該世代以降の世代管理復号キーの取得を実行するキー取得ステップと、

の少なくともいずれかを実行するステップ

を有することを特徴とするプログラム提供媒体。

１００．　前記コンピュータ・プログラムは、さらに、

複数の異なる情報再生装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報再生装置固有のリーフキーの少なくともいずれかを用いて記録媒体に格納された暗号データの復号処理を実行する世代管理復号キーの更新処理を実行する更新ステップを含むことを特徴とする請求の範囲第９９項に記載のプログラム提供媒体。

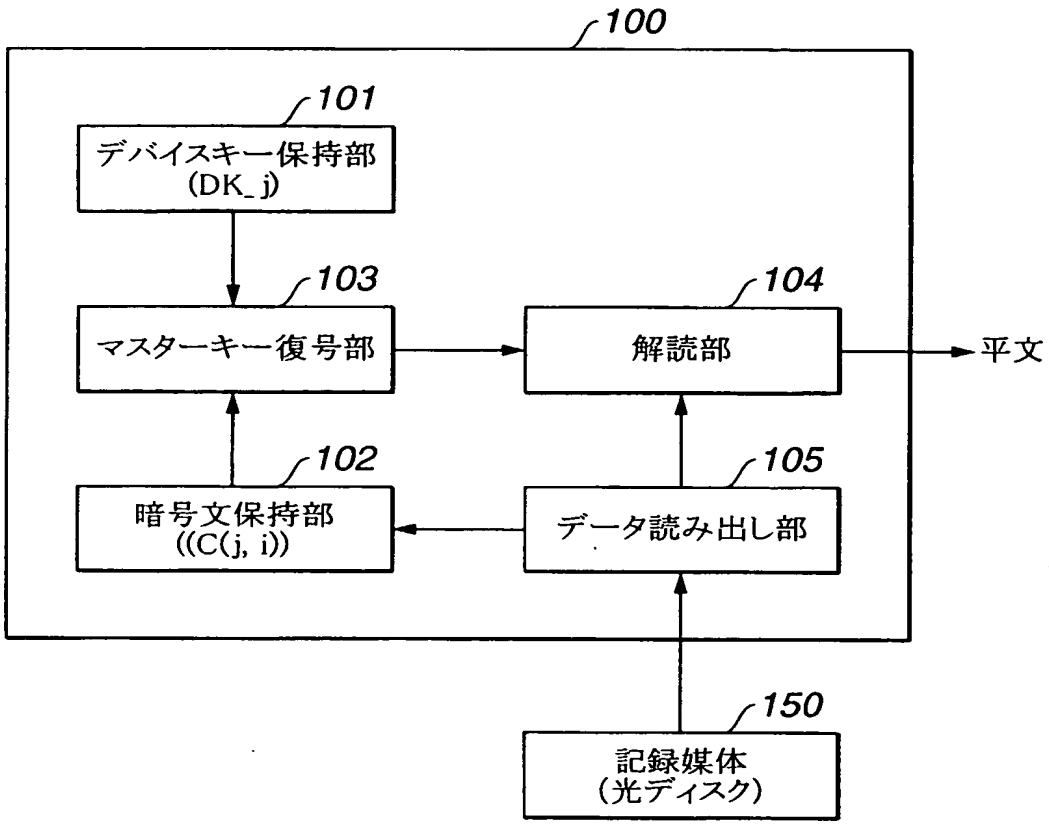
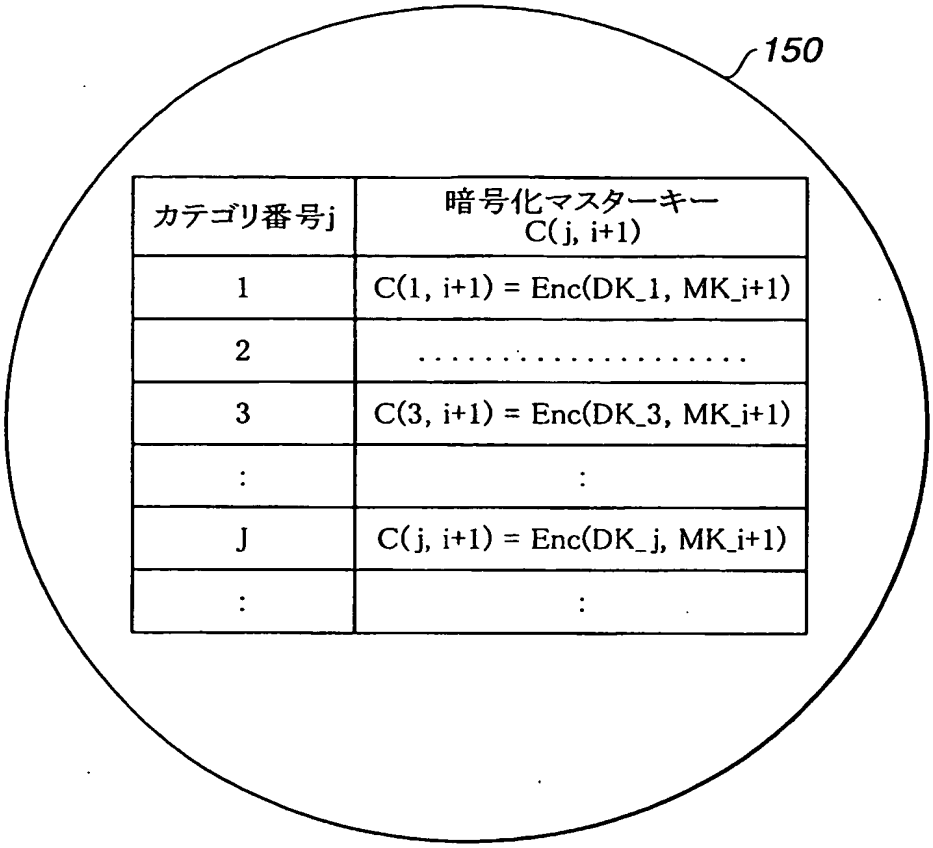

100
101
デバイスキー保持部
(DK_j)
103
マスターキー復号部
104
解読部
平文
102
暗号文保持部
((C(j, i))
105
データ読み出し部
150
記録媒体
(光ディスク)

FIG.1



カテゴリ番号j	暗号化マスターキー C(j, i+1)
1	C(1, i+1) = Enc(DK_1, MK_i+1)
2	.....
3	C(3, i+1) = Enc(DK_3, MK_i+1)
:	:
J	C(j, i+1) = Enc(DK_j, MK_i+1)
:	:

FIG.2

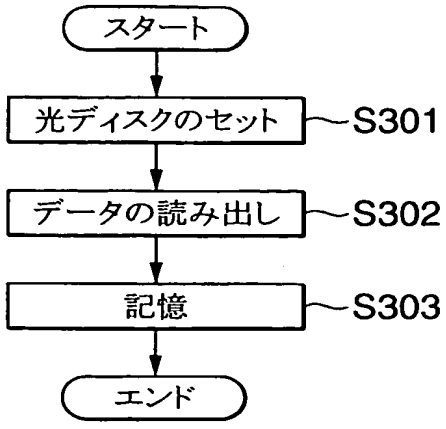


FIG.3

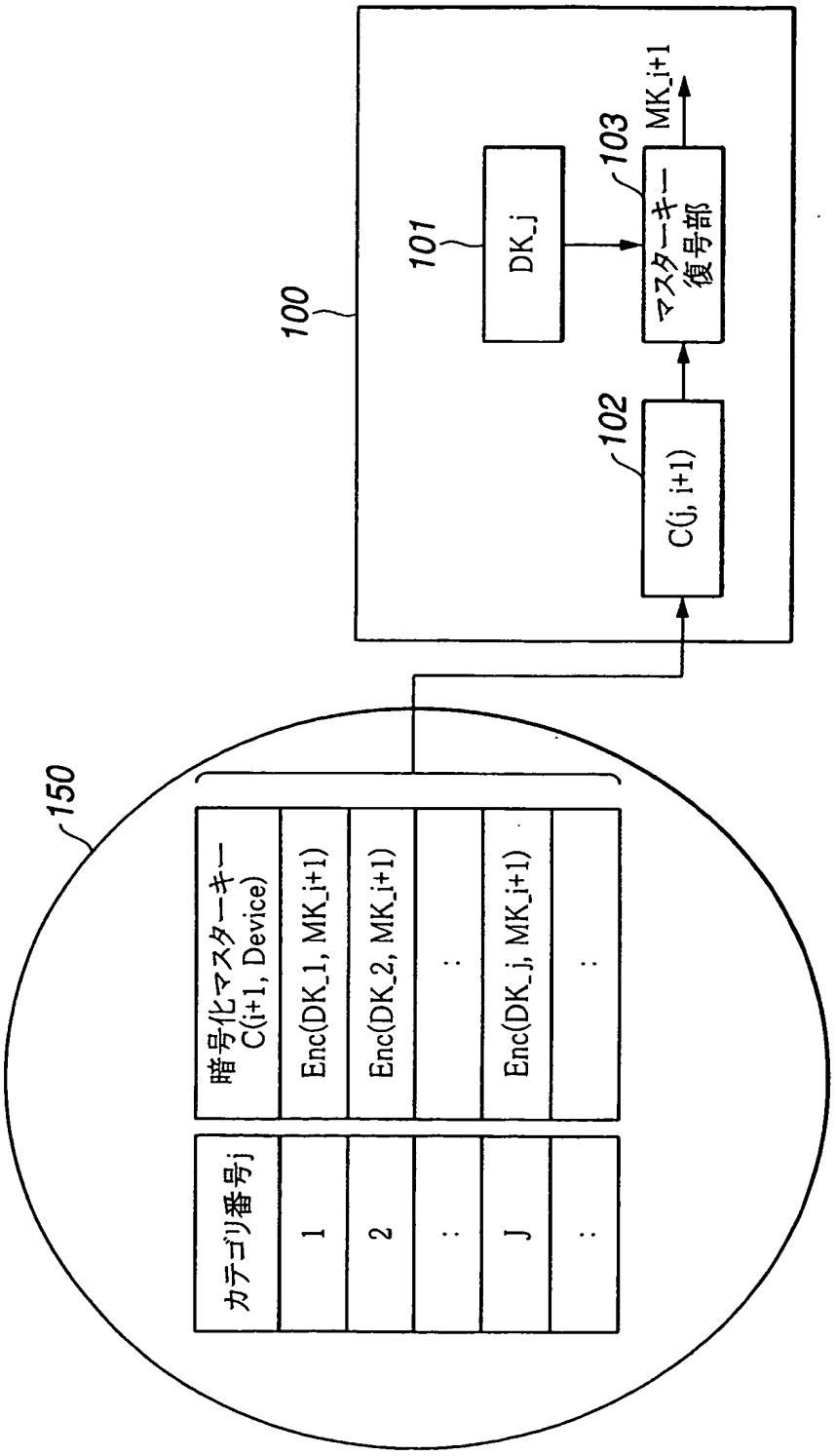

150
カテゴリ番号j
暗号化マスターキー C(i+1, Device)
1
Enc(DK_1, MK_i+1)
2
Enc(DK_2, MK_i+1)
J
Enc(DK_j, MK_i+1)
100
101
DK_j
102
C(j, i+1)
103
マスターキー復号部
MK_i+1

FIG.4

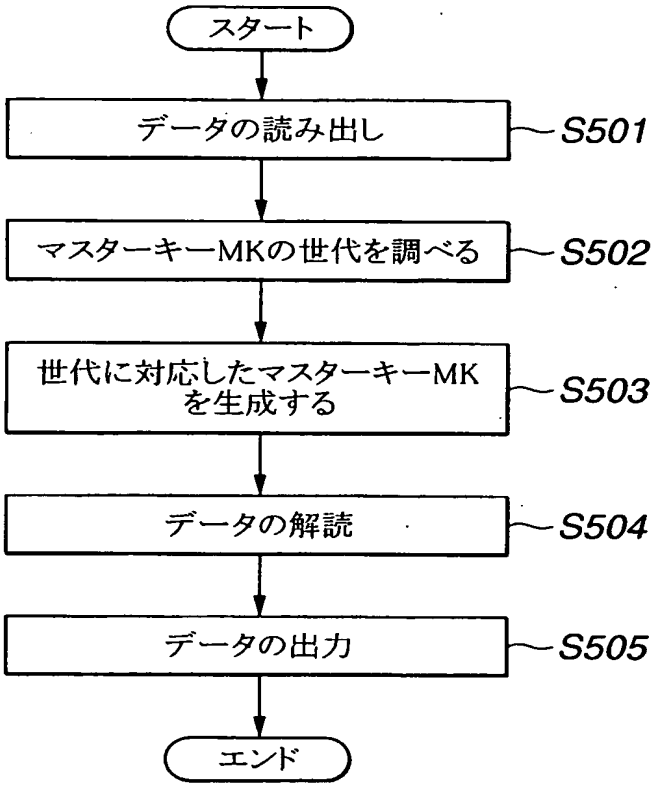

スタート
データの読み出し
S501
マスターキーMKの世代を調べる
S502
世代に対応したマスターキーMK
を生成する
S503
データの解読
S504
データの出力
S505
エンド

FIG.5

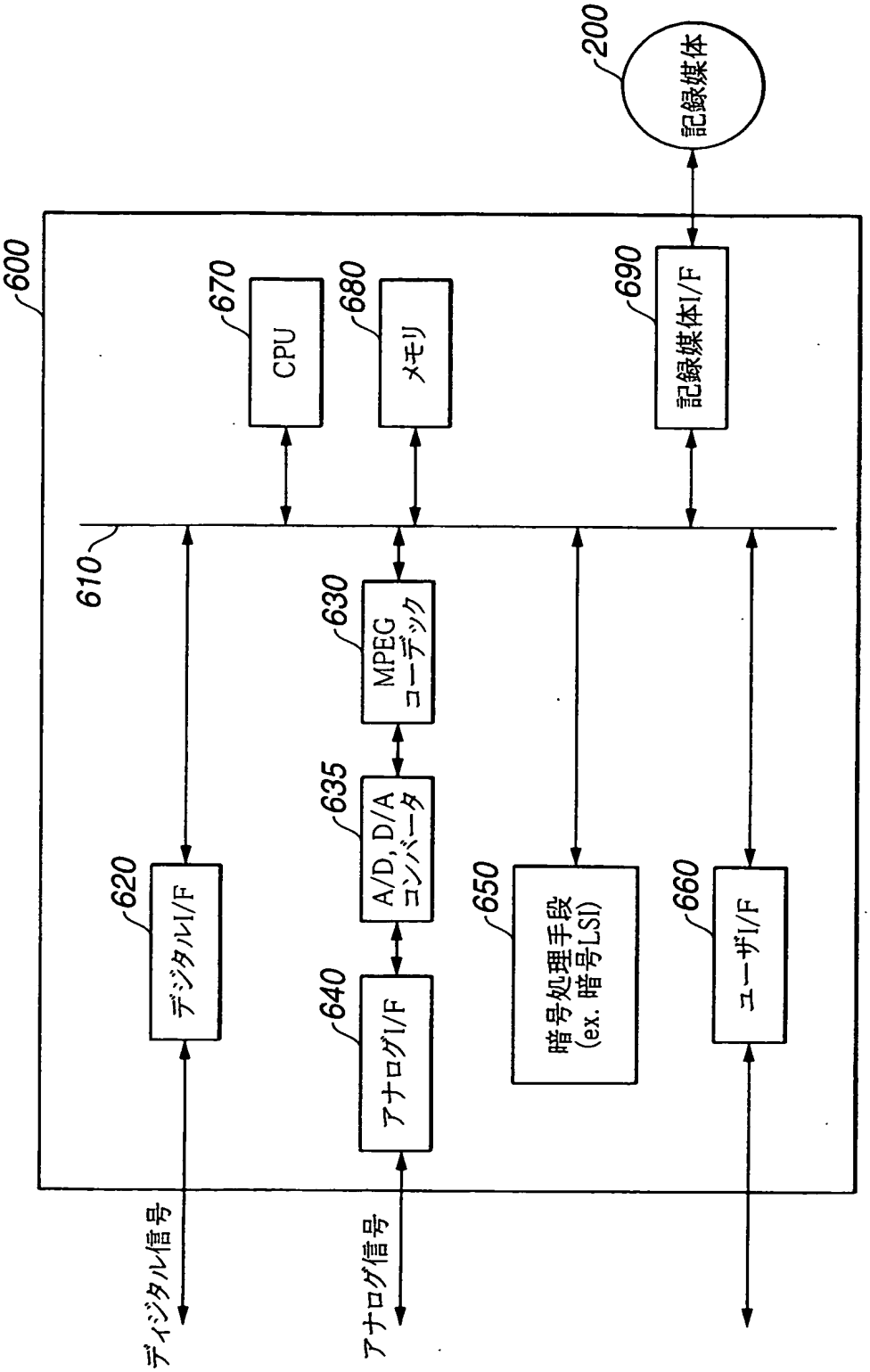

200
記録媒体
600
670
CPU
680
メモリ
690
記録媒体I/F
610
630
MPEG
コーデック
635
A/D, D/A
コンバータ
620
デジタルI/F
640
アナログI/F
650
暗号処理手段
(ex. 暗号LSI)
660
ユーザI/F
ディジタル信号
アナログ信号

FIG.6

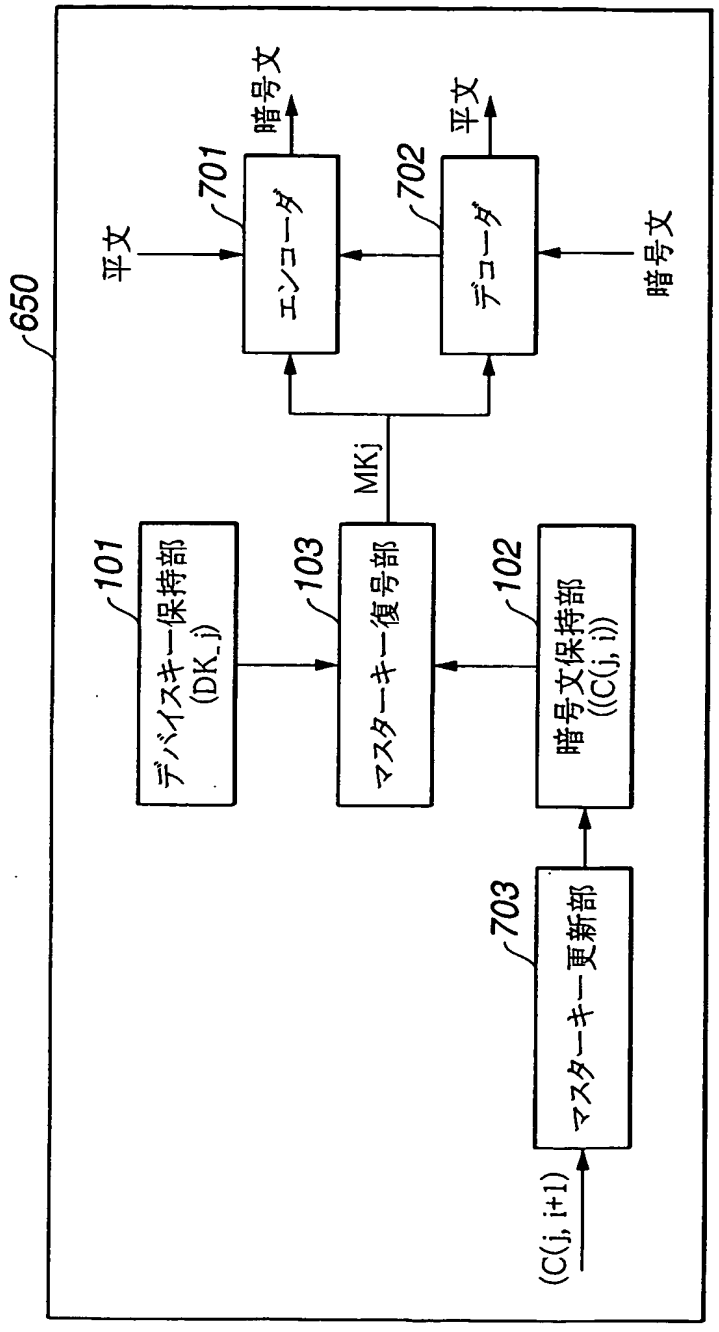

650
平文
701
エンコーダ
暗号文
暗号文
702
デコーダ
平文
MKj
101
デバイスキー保持部
(DK_j)
103
マスターキー復号部
102
暗号文保持部
((C(j, i))
703
マスターキー更新部
(C(j, i+1)

FIG.7

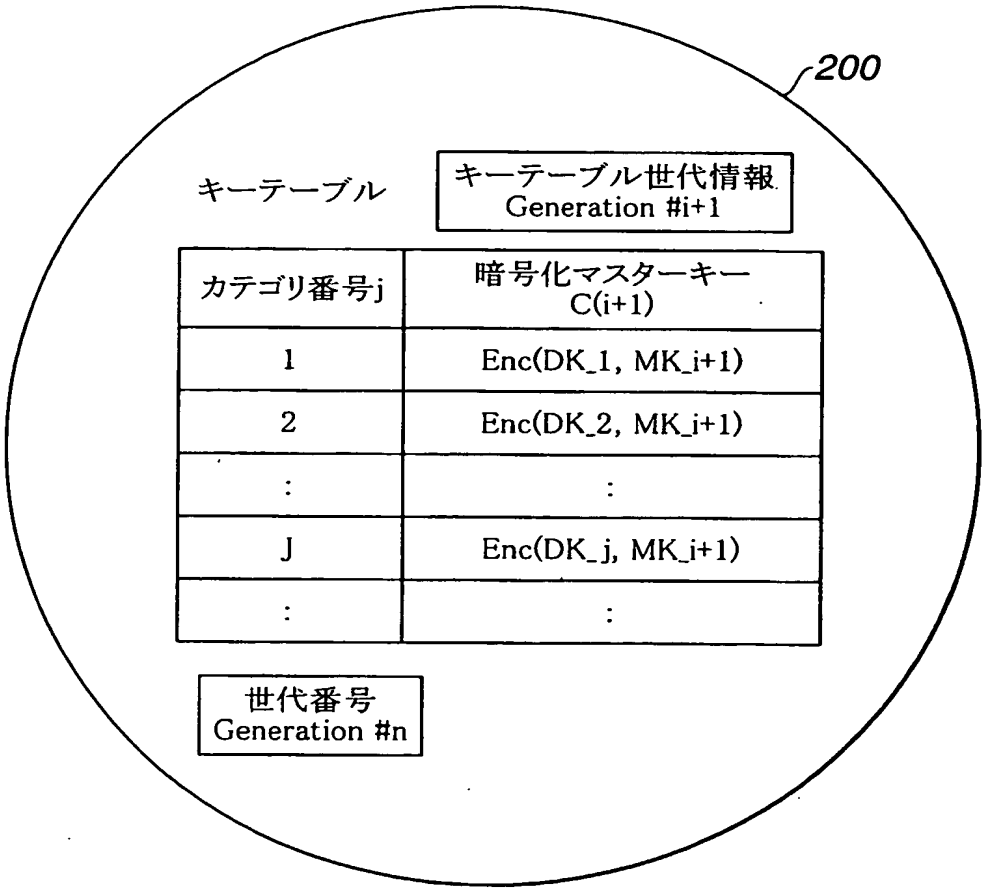

200
キーテーブル
キーテーブル世代情報
Generation #i+1
カテゴリ番号j
暗号化マスターキー
C(i+1)
1
Enc(DK_1, MK_i+1)
2
Enc(DK_2, MK_i+1)
:
:
J
Enc(DK_j, MK_i+1)
:
:
世代番号
Generation #n

FIG.8

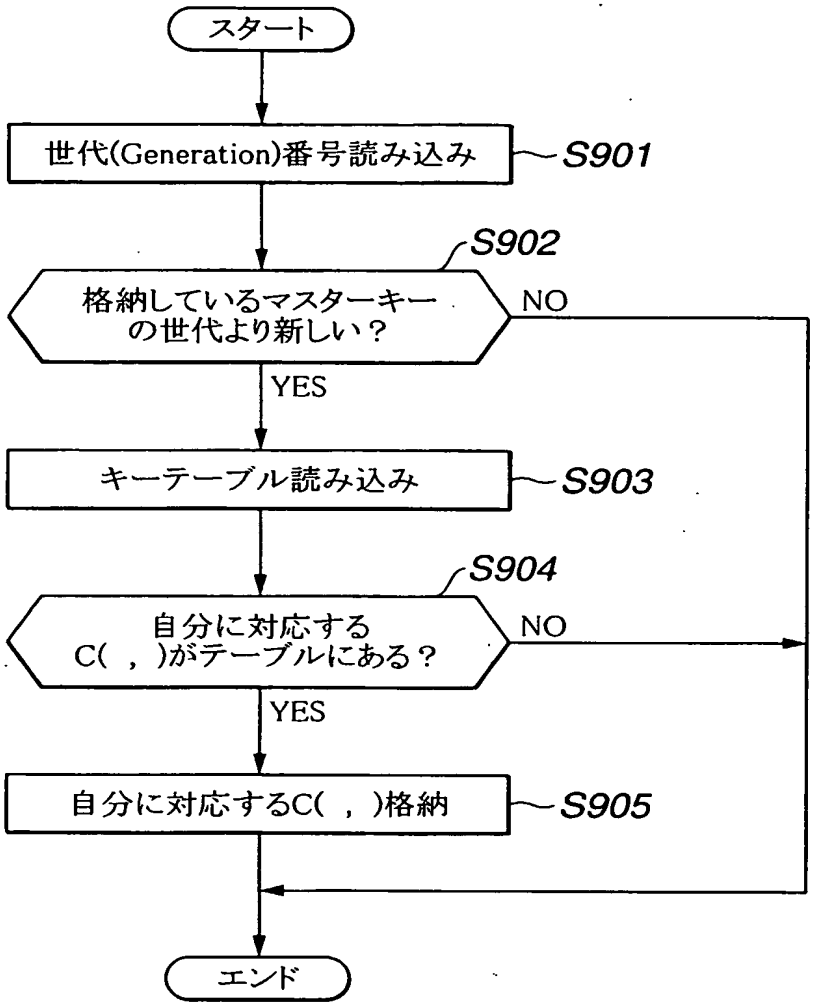

スタート
世代(Generation)番号読み込み
S901
S902
格納しているマスターキーの世代より新しい？
NO
YES
キーテーブル読み込み
S903
S904
自分に対応するC(,)がテーブルにある？
NO
YES
自分に対応するC(,)格納
S905
エンド

FIG.9

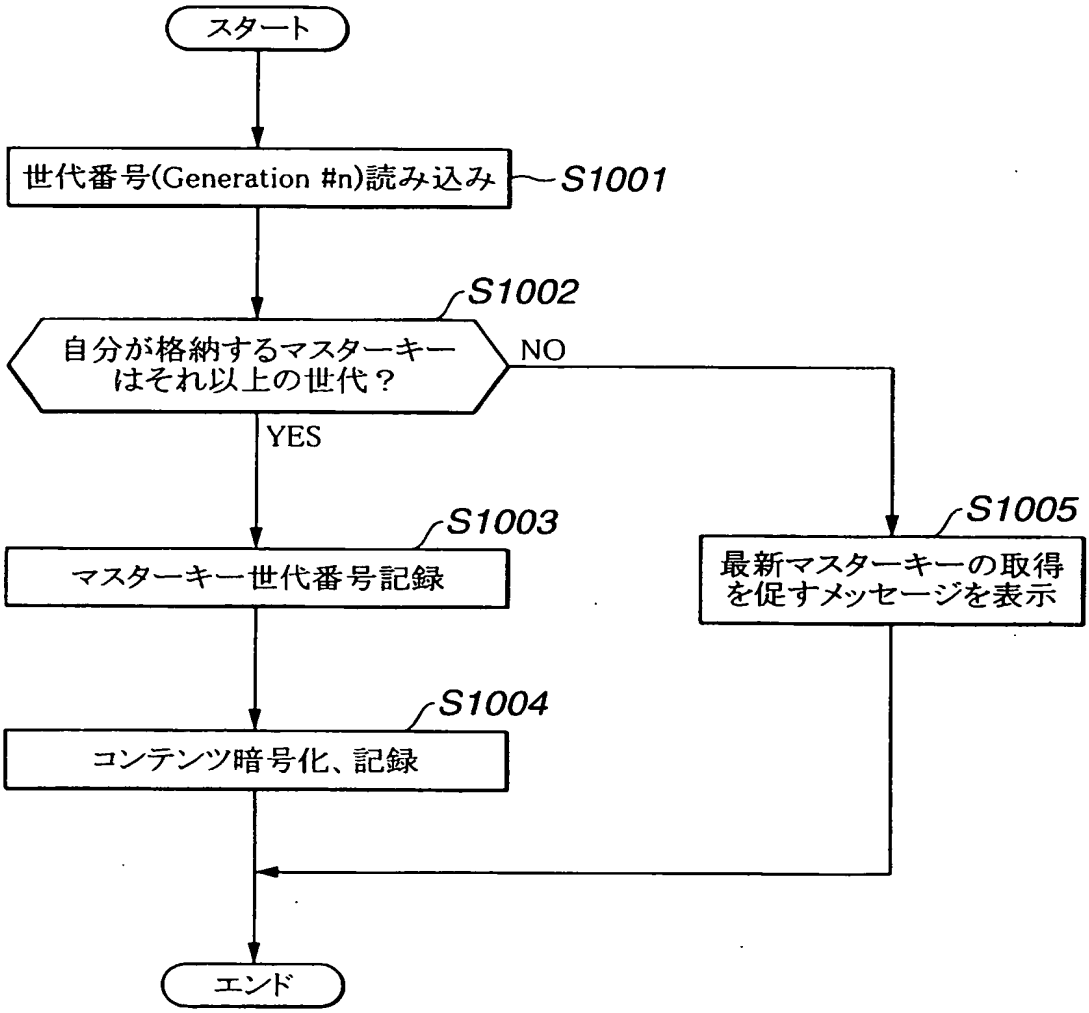

スタート
世代番号(Generation #n)読み込み
S1001
S1002
自分が格納するマスターキー
はそれ以上の世代？
NO
YES
S1003
マスターキー世代番号記録
S1005
最新マスターキーの取得
を促すメッセージを表示
S1004
コンテンツ暗号化、記録
エンド

FIG.10

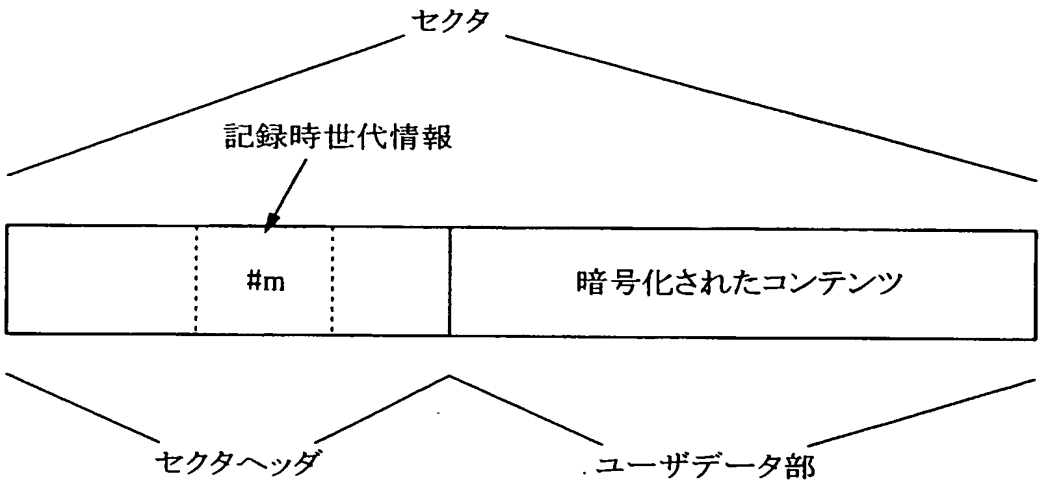


FIG.11

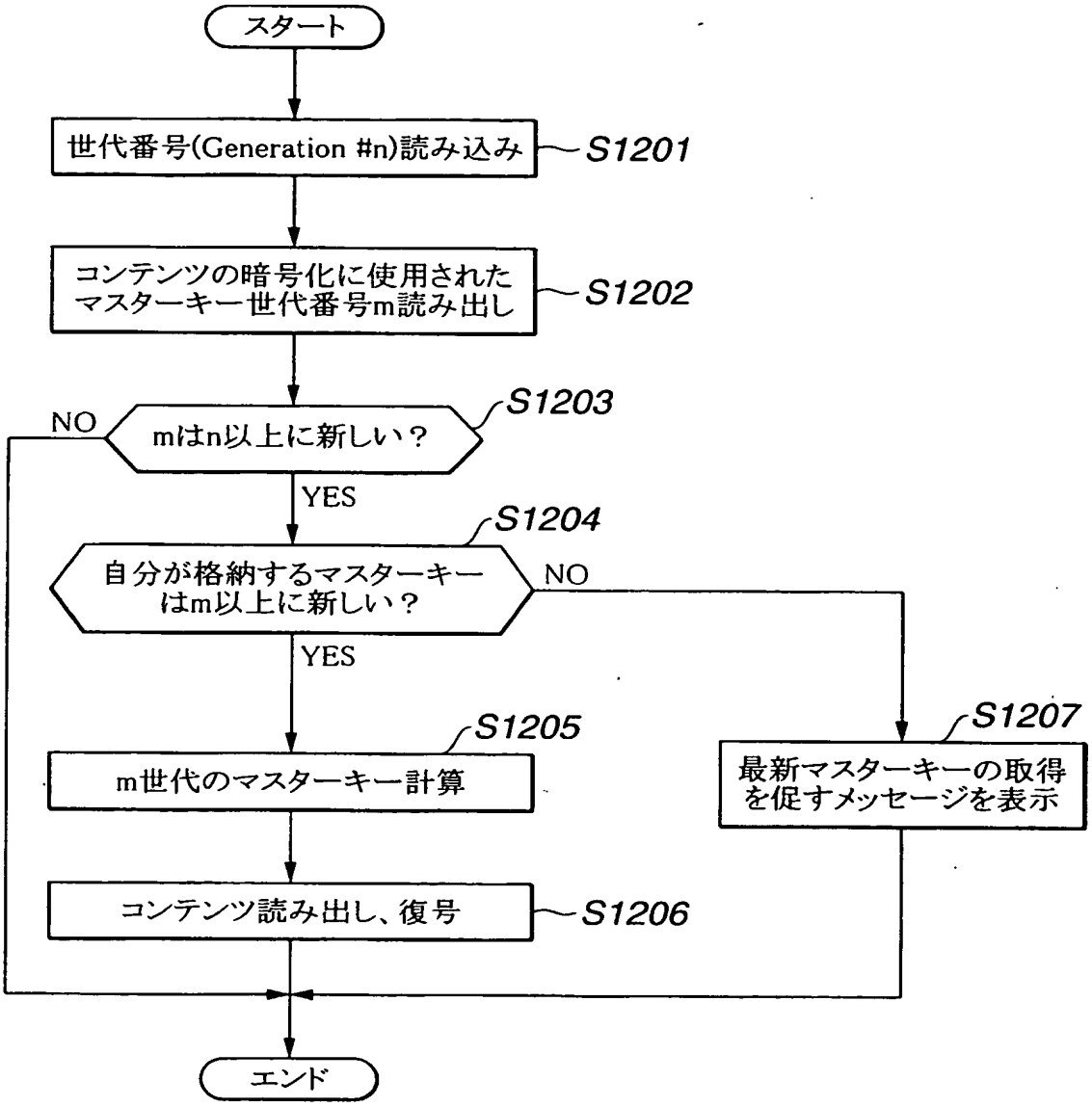

スタート
世代番号(Generation #n)読み込み
S1201
コンテンツの暗号化に使用された
マスターキー世代番号m読み出し
S1202
S1203
NO
mはn以上に新しい？
YES
S1204
自分が格納するマスターキー
はm以上に新しい？
NO
YES
S1205
m世代のマスターキー計算
S1207
最新マスターキーの取得
を促すメッセージを表示
コンテンツ読み出し、復号
S1206
エンド

FIG.12

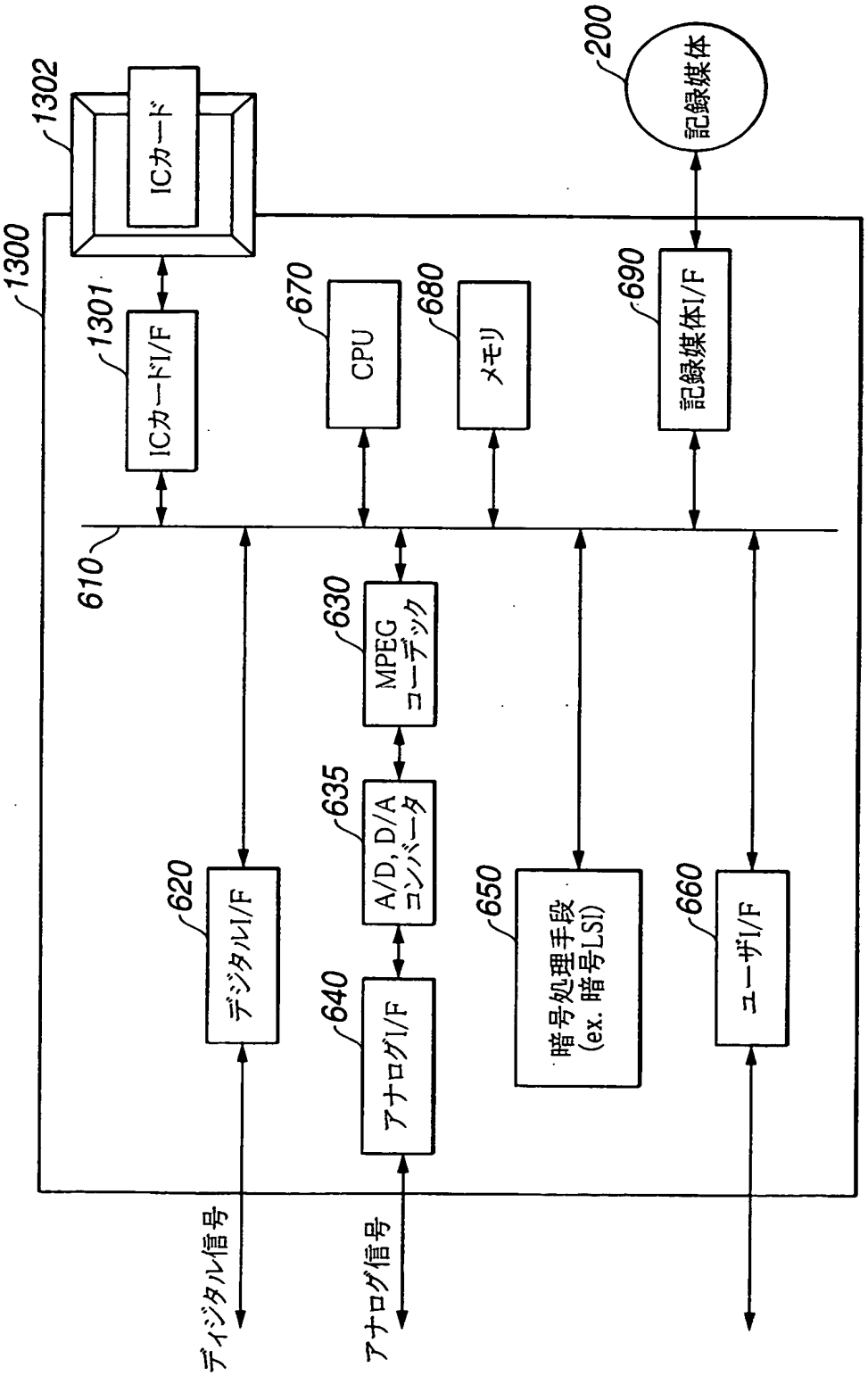

1300
1301
ICカードI/F
1302
ICカード
200
記録媒体
670
CPU
680
メモリ
690
記録媒体I/F
610
630
MPEG
コーデック
635
A/D, D/A
コンバータ
620
デジタルI/F
640
アナログI/F
650
暗号処理手段
(ex. 暗号LSI)
660
ユーザI/F
ディジタル信号
アナログ信号

FIG.13

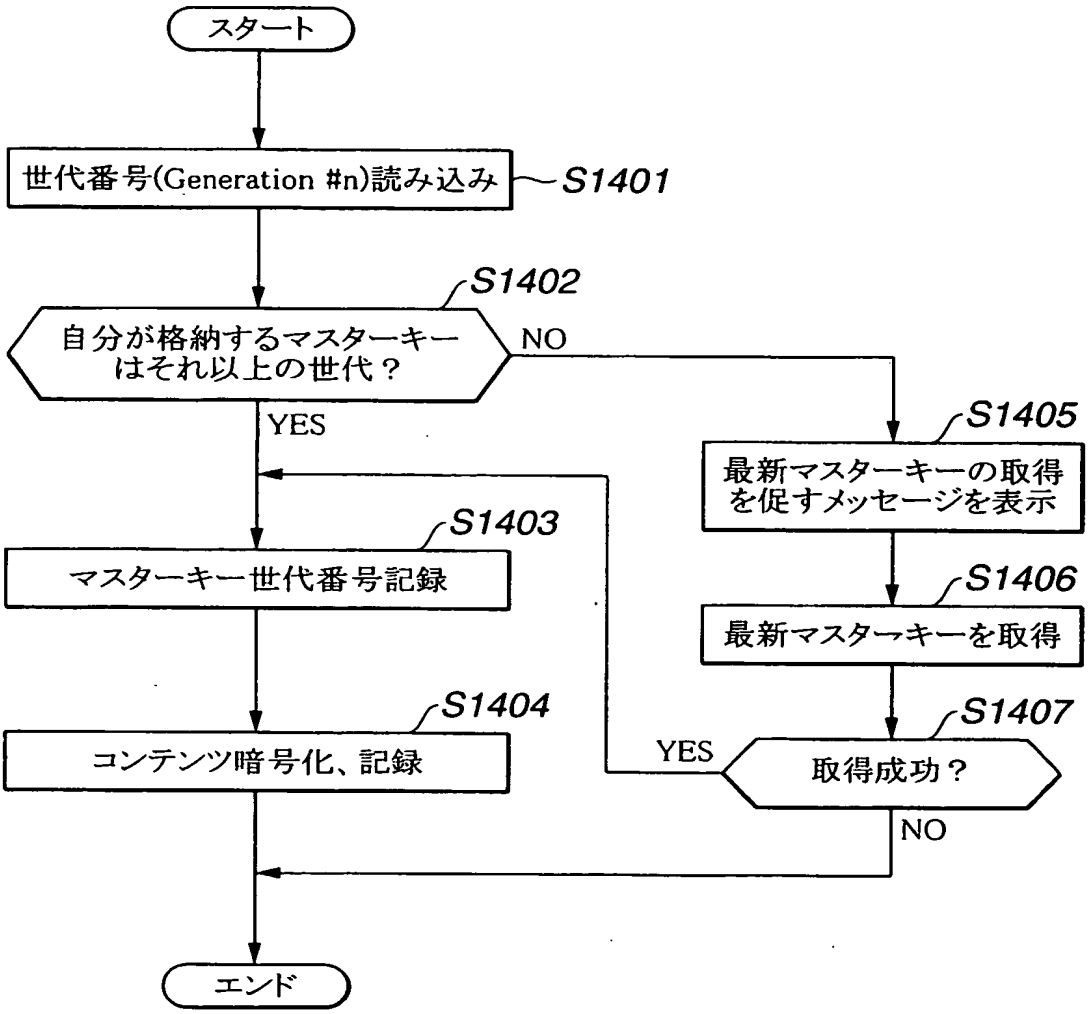

スタート
世代番号(Generation #n)読み込み
S1401
S1402
自分が格納するマスターキー
はそれ以上の世代？
NO
YES
S1405
最新マスターキーの取得
を促すメッセージを表示
S1403
マスターキー世代番号記録
S1406
最新マスターキーを取得
S1404
コンテンツ暗号化、記録
S1407
YES
取得成功？
NO
エンド

FIG.14

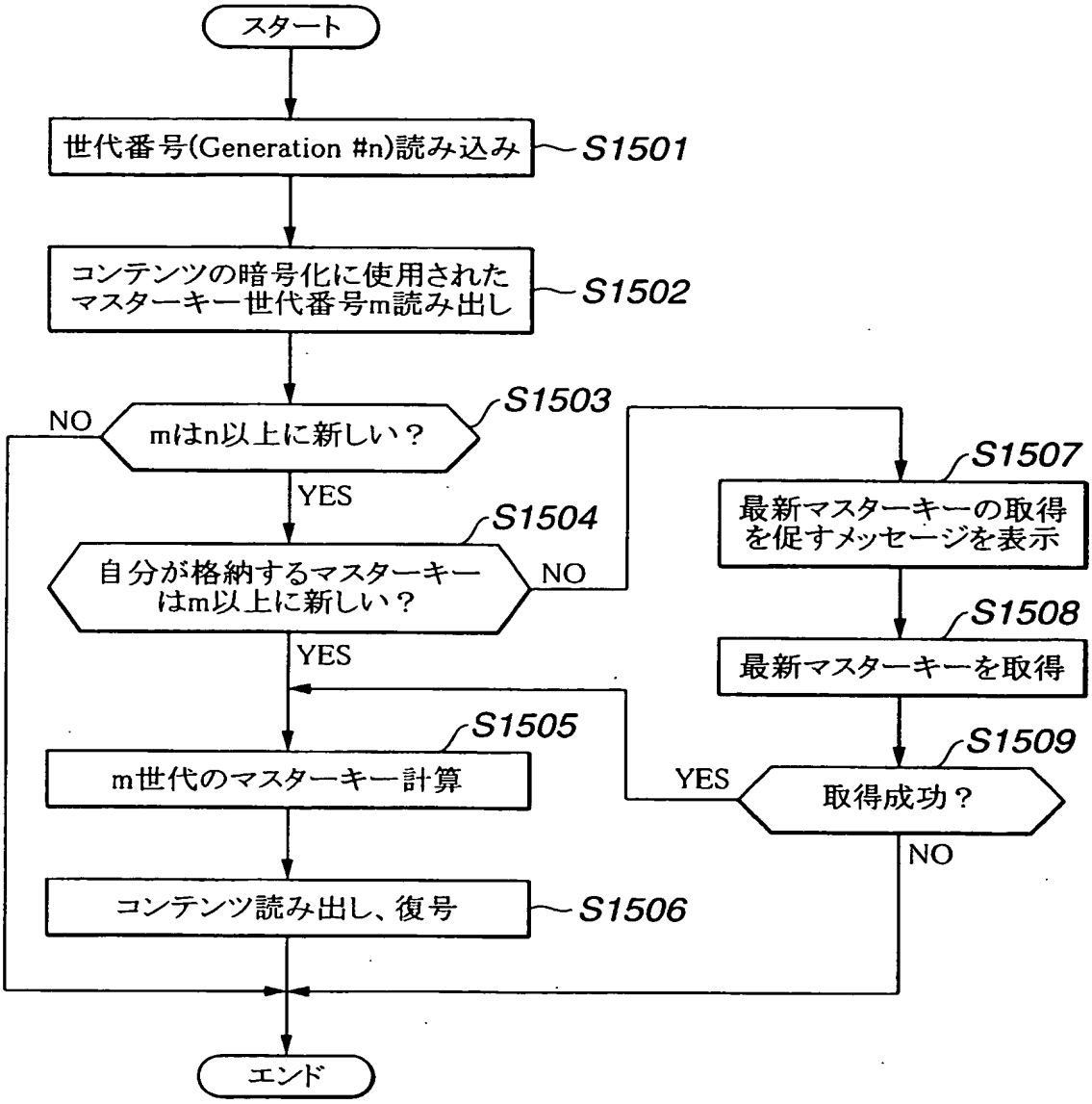

スタート
世代番号(Generation #n)読み込み
S1501
コンテンツの暗号化に使用された
マスターキー世代番号m読み出し
S1502
S1503
NO
mはn以上に新しい？
YES
S1504
自分が格納するマスターキー
はm以上に新しい？
NO
YES
S1505
m世代のマスターキー計算
コンテンツ読み出し、復号
S1506
S1507
最新マスターキーの取得
を促すメッセージを表示
S1508
最新マスターキーを取得
S1509
YES
取得成功？
NO
エンド

FIG.15

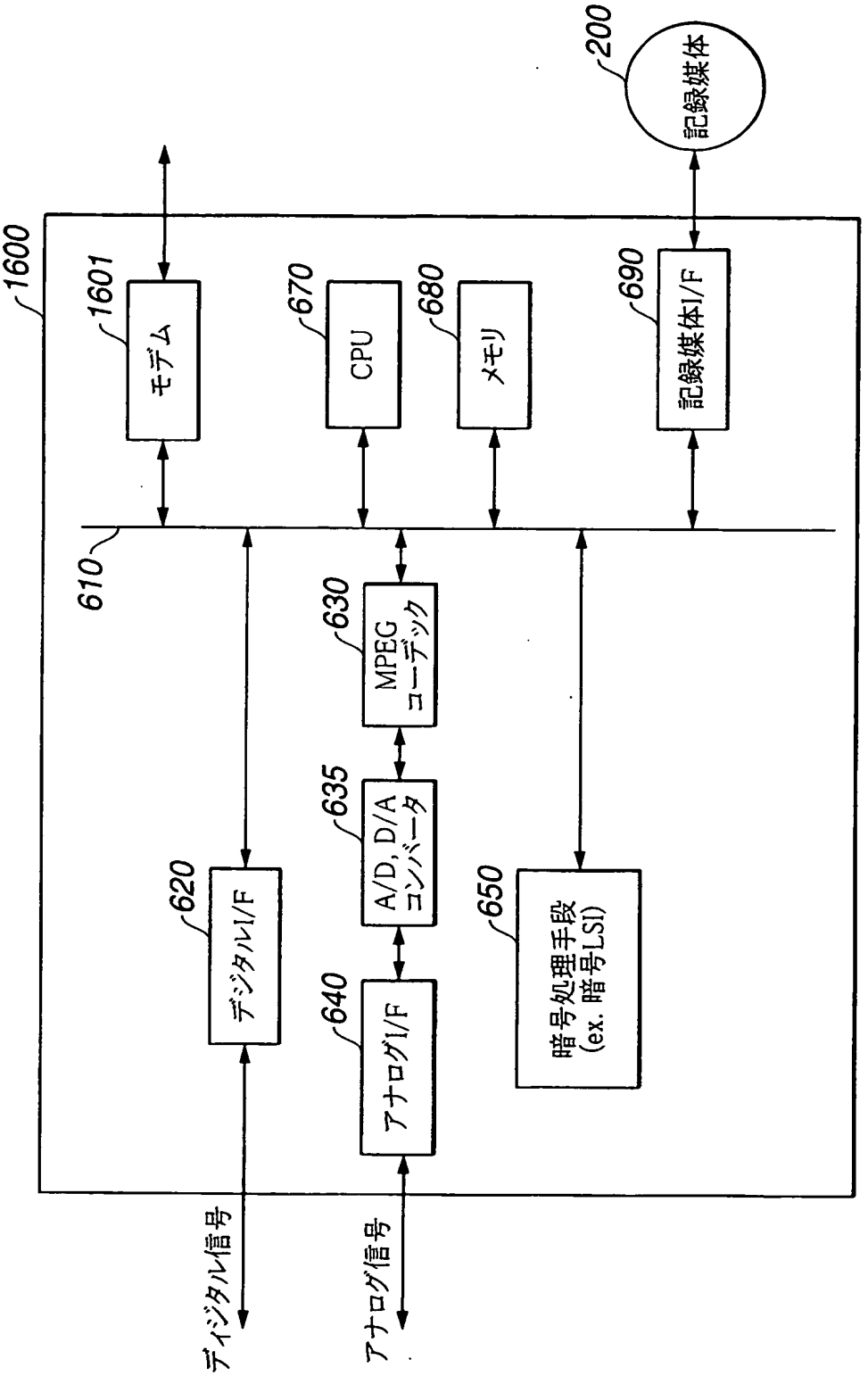

200
記録媒体
1600
1601
モデム
670
CPU
680
メモリ
690
記録媒体I/F
610
630
MPEG
コーデック
635
A/D, D/A
コンバータ
620
デジタルI/F
640
アナログI/F
650
暗号処理手段
(ex. 暗号LSI)
ディジタル信号
アナログ信号

FIG.16

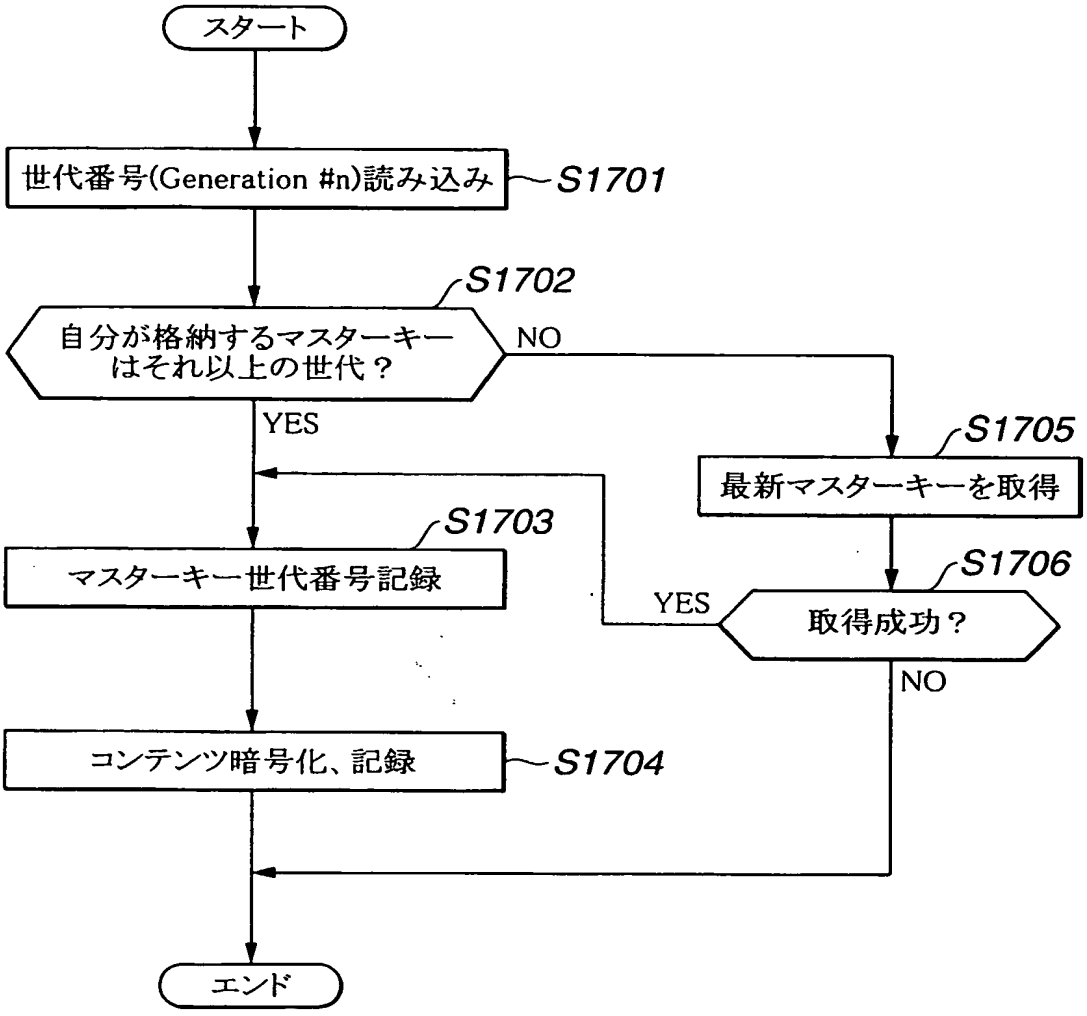

スタート
世代番号(Generation #n)読み込み
S1701
S1702
自分が格納するマスターキーはそれ以上の世代？
NO
YES
S1705
最新マスターキーを取得
S1703
マスターキー世代番号記録
S1706
YES
取得成功？
NO
コンテンツ暗号化、記録
S1704
エンド

FIG.17

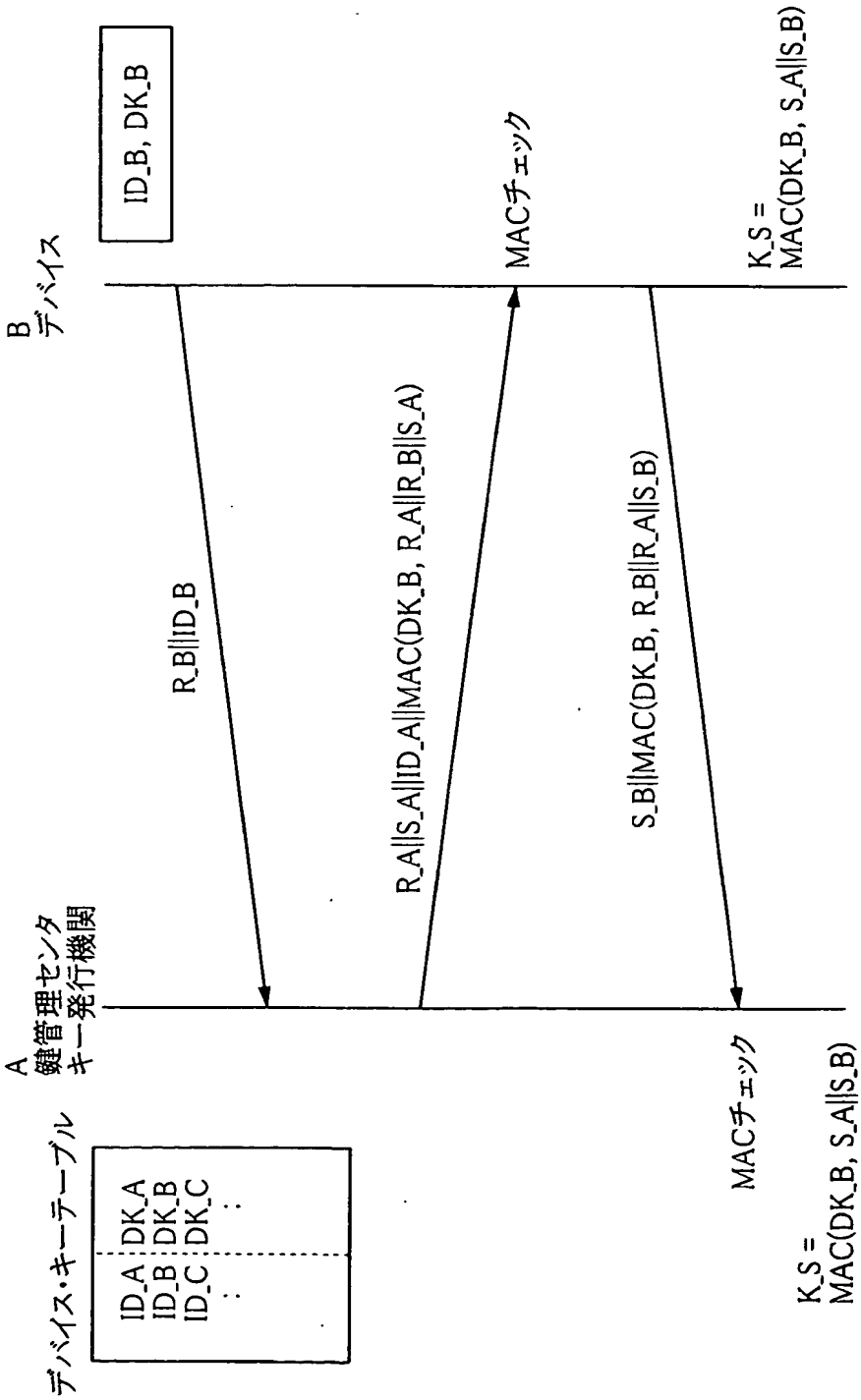

B
デバイス
ID_B, DK_B
MACチェック
K_S =
MAC(DK_B, S_A||S_B)
R_B||ID_B
R_A||S_A||ID_A||MAC(DK_B, R_A||R_B||S_A)
S_B||MAC(DK_B, R_B||R_A||S_B)
A
鍵管理センタ
キー発行機関
デバイス・キーテーブル
ID_A DK_A
ID_B DK_B
ID_C DK_C
MACチェック
K_S =
MAC(DK_B, S_A||S_B)

FIG.18

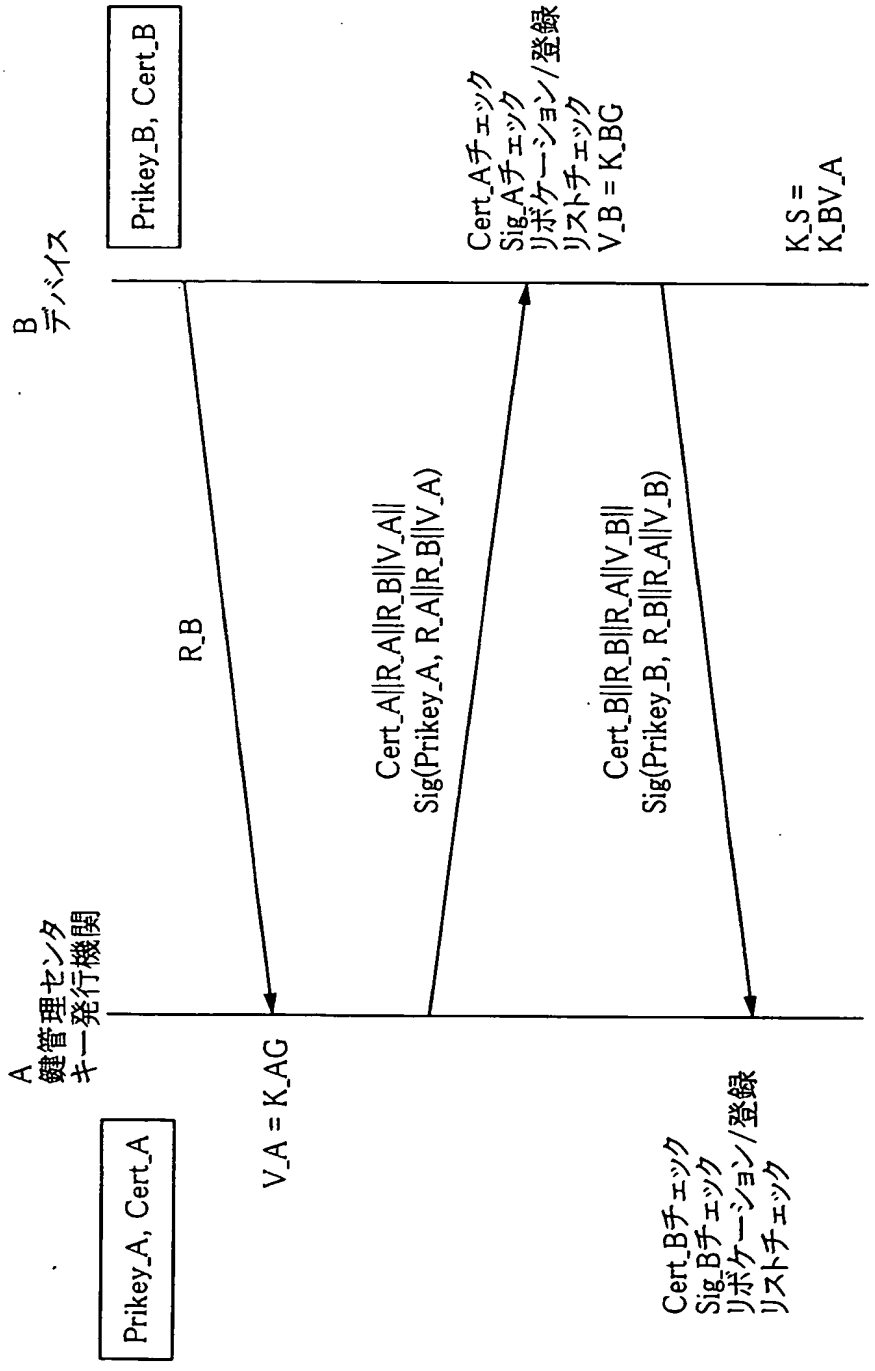

B
デバイス
Prikey_B, Cert_B
R_B
Cert_A||R_A||R_B||V_A||
Sig(Prikey_A, R_A||R_B||V_A)
Cert_Aチェック
Sig_Aチェック
リボケーション/登録
リストチェック
V_B = K_BG
K_S =
K_BV_A
Cert_B||R_B||R_A||V_B||
Sig(Prikey_B, R_B||R_A||V_B)
A
鍵管理センタ
キー発行機関
Prikey_A, Cert_A
V_A = K_AG
Cert_Bチェック
Sig_Bチェック
リボケーション/登録
リストチェック
K_S =
K_AV_B

FIG.19

BのID(ID_B)
Bの公開鍵(Pubkey_B)
上記の全フィールドに対するセンタのデジタル署名

FIG.20

バージョンナンバ
リボークされる機器のID
:
センタのデジタル署名

FIG.21

バージョンナンバ
登録される機器のID
:
センタのデジタル署名

FIG.22

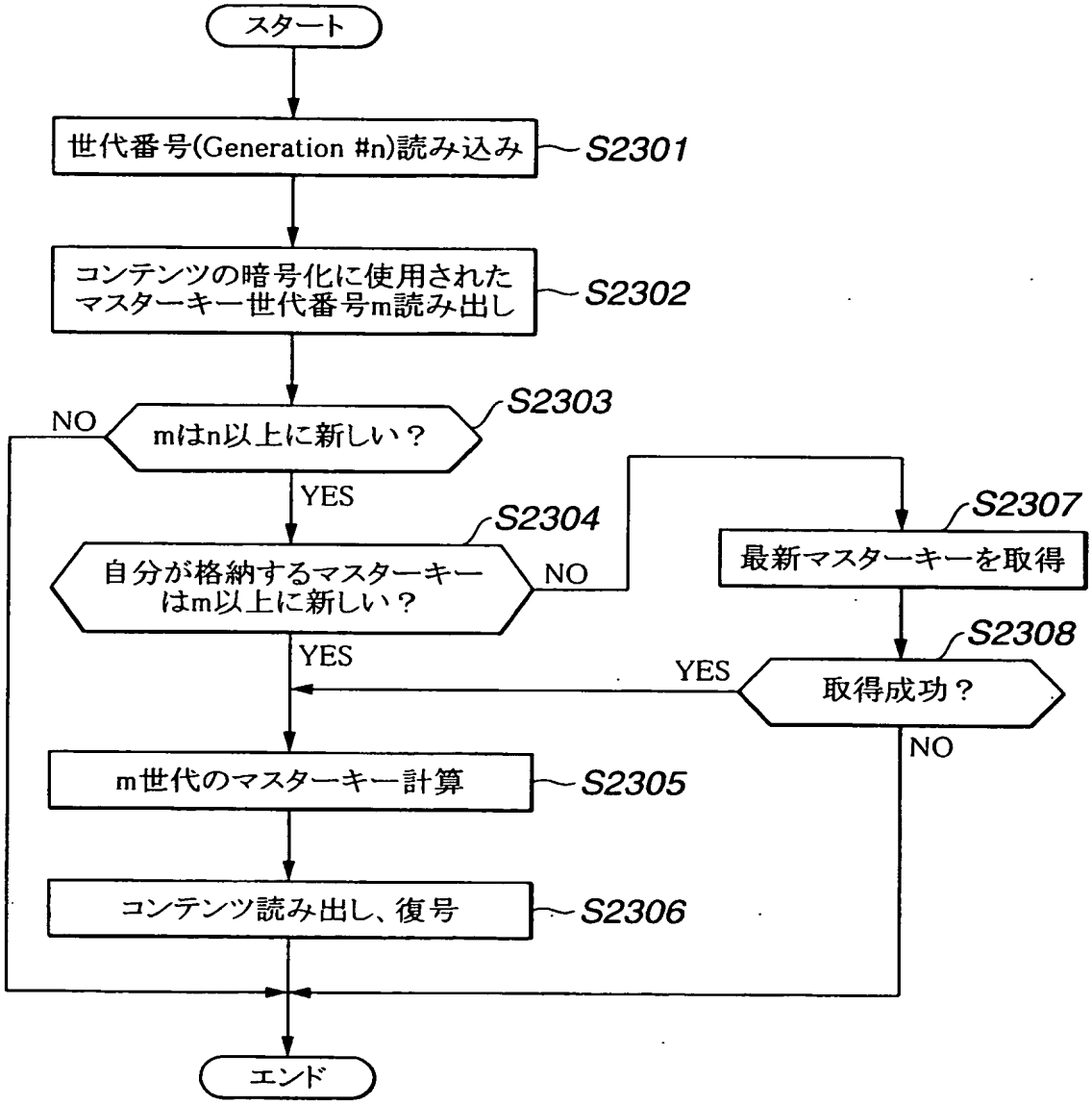

スタート
世代番号(Generation #n)読み込み
S2301
コンテンツの暗号化に使用された
マスターキー世代番号m読み出し
S2302
S2303
NO
mはn以上に新しい？
YES
S2304
自分が格納するマスターキー
はm以上に新しい？
NO
S2307
最新マスターキーを取得
S2308
YES
YES
取得成功？
NO
m世代のマスターキー計算
S2305
コンテンツ読み出し、復号
S2306
エンド

FIG.23

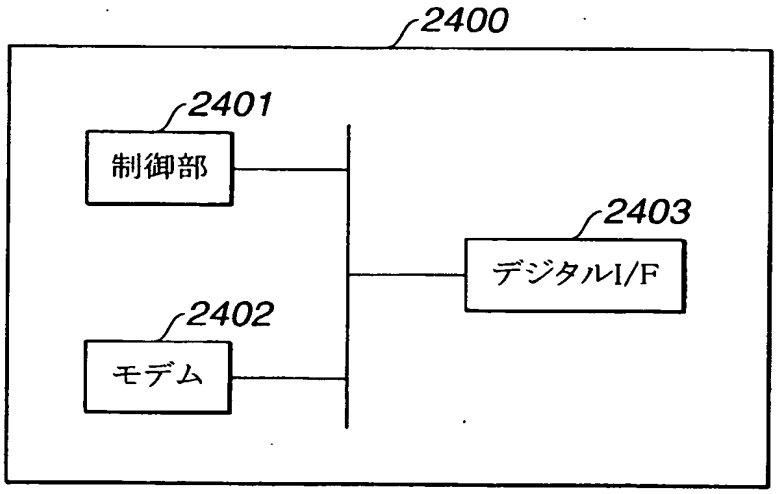


FIG.24

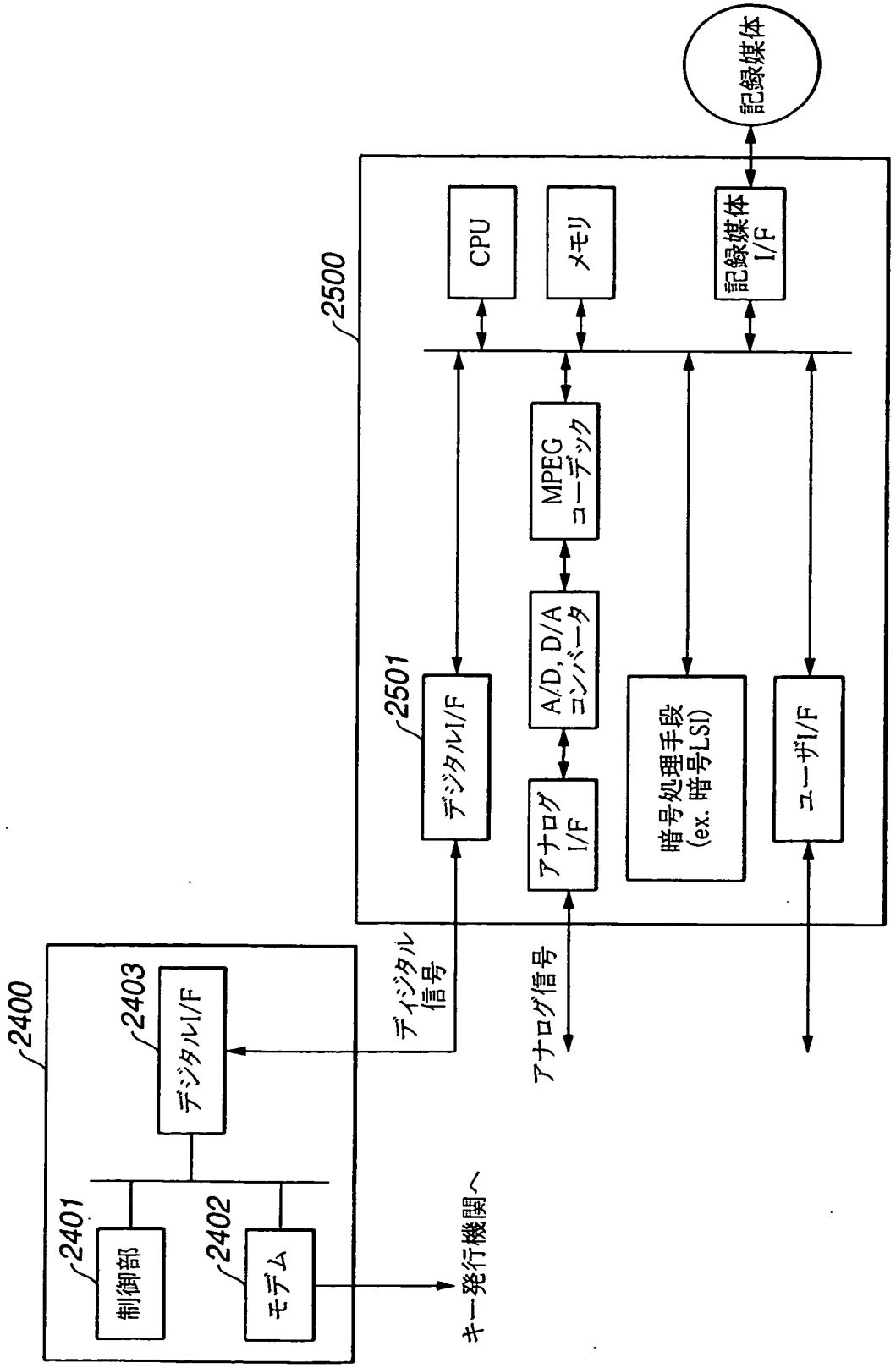

記録媒体
2500
CPU
メモリ
記録媒体I/F
MPEGコーデック
A/D, D/Aコンバータ
2501
デジタルI/F
アナログI/F
暗号処理手段(ex. 暗号LSI)
ユーザI/F
デジタル信号
アナログ信号
2400
2403
デジタルI/F
2401
制御部
2402
モデム
キー発行機関へ

FIG.25

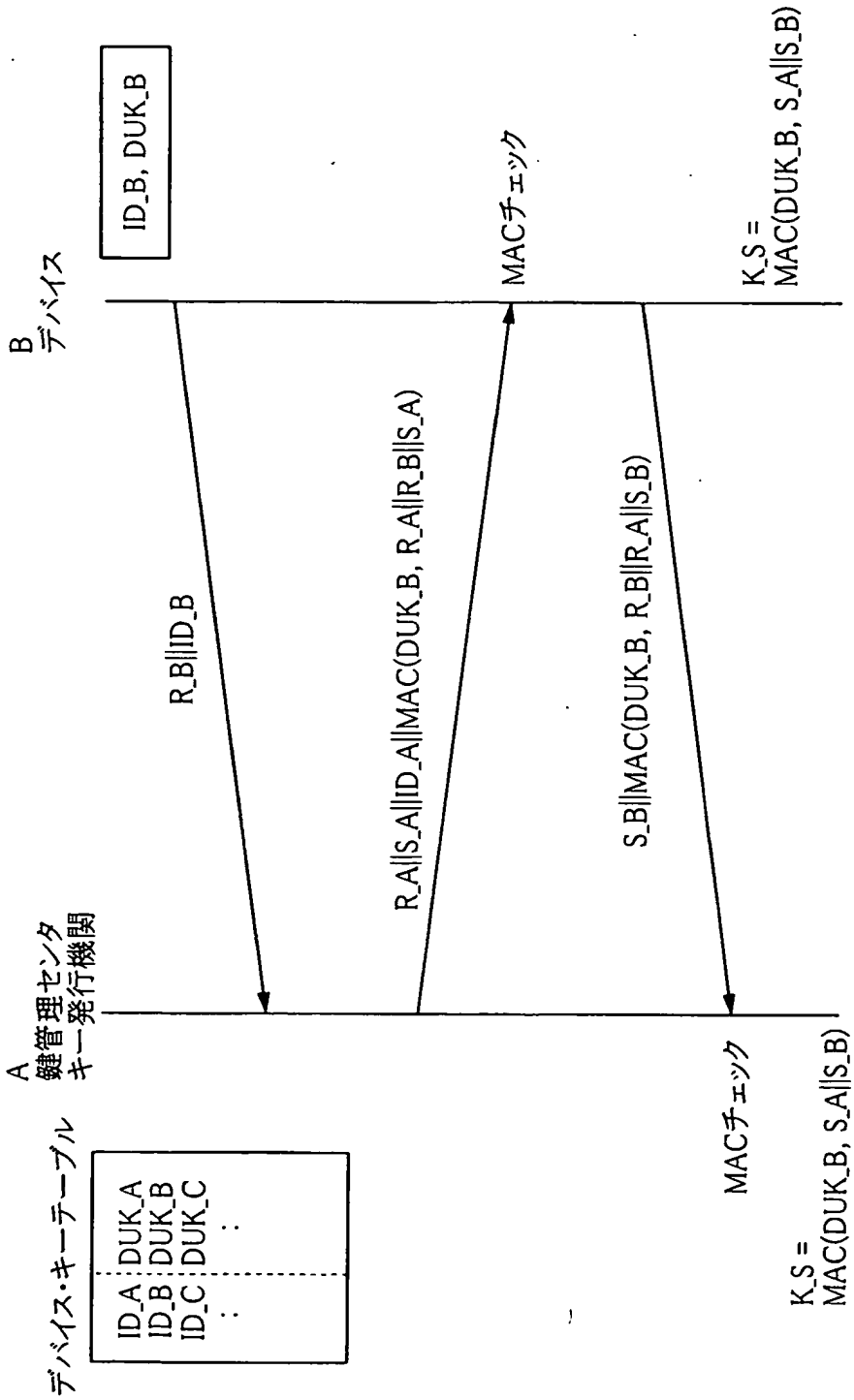

B
デバイス
ID_B, DUK_B
MACチェック
K_S =
MAC(DUK_B, S_A||S_B)
R_B||ID_B
R_A||S_A||ID_A||MAC(DUK_B, R_A||R_B||S_A)
S_B||MAC(DUK_B, R_B||R_A||S_B)
A
鍵管理センタ
キー発行機関
デバイス・キーテーブル
ID_A DUK_A
ID_B DUK_B
ID_C DUK_C
MACチェック
K_S =
MAC(DUK_B, S_A||S_B)

FIG.26

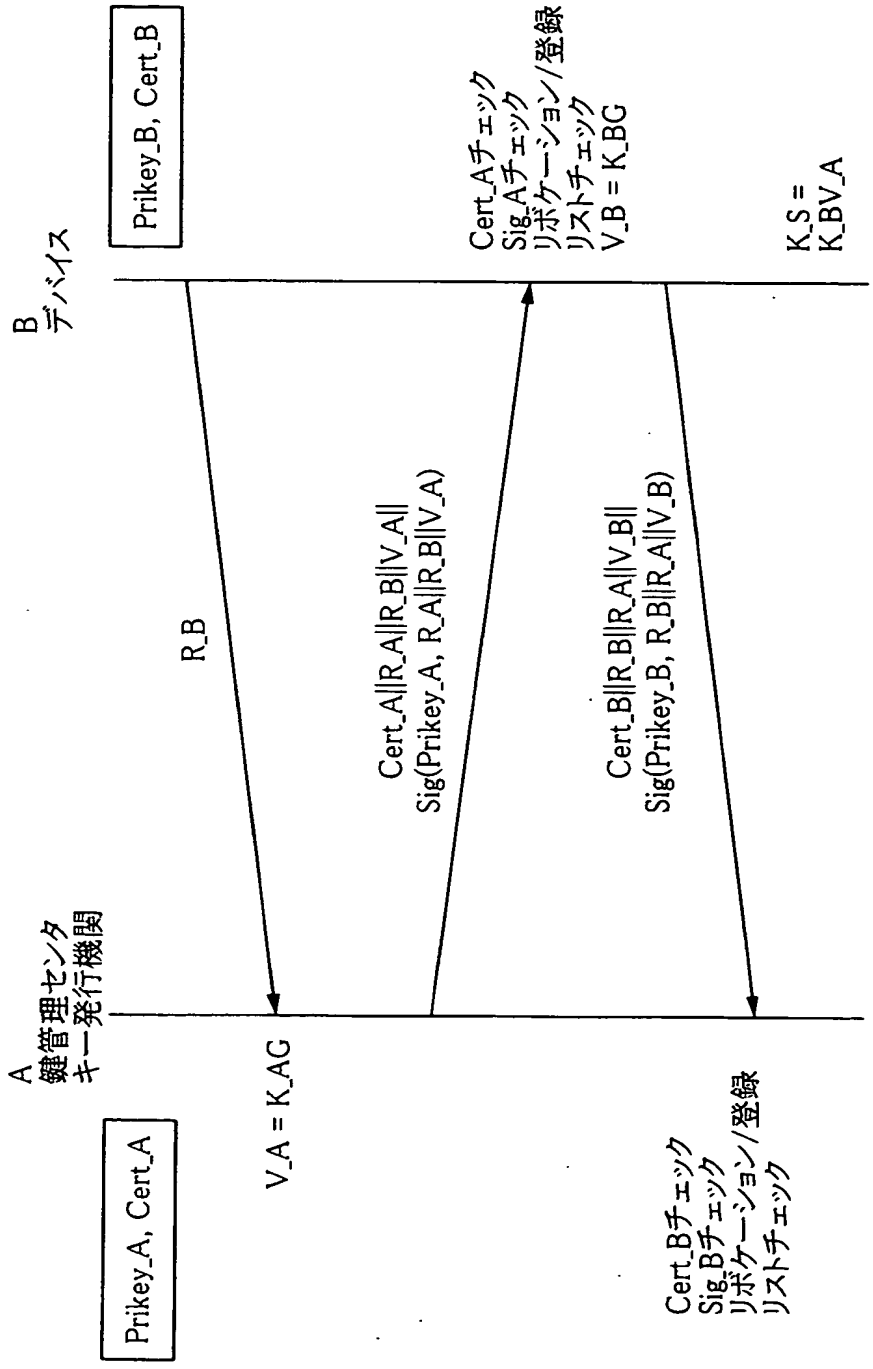

A
鍵管理センタ
キー発行機関
Prikey_A, Cert_A
B
デバイス
Prikey_B, Cert_B
R_B
V_A = K_AG
Cert_A||R_A||R_B||V_A||
Sig(Prikey_A, R_A||R_B||V_A)
Cert_Aチェック
Sig_Aチェック
リボケーション/登録
リストチェック
V_B = K_BG
K_S =
K_BV_A
Cert_B||R_B||R_A||V_B||
Sig(Prikey_B, R_B||R_A||V_B)
Cert_Bチェック
Sig_Bチェック
リボケーション/登録
リストチェック
K_S =
K_AV_B

FIG.27

世代番号#n	
装置固有識別番号(機器ID)	暗号化マスターキー
1	Enc(DUK_1, MK_n)
2	Enc(DUK_2, MK_n)
:	:
L	Enc(DUK_L, MK_n)

FIG.28

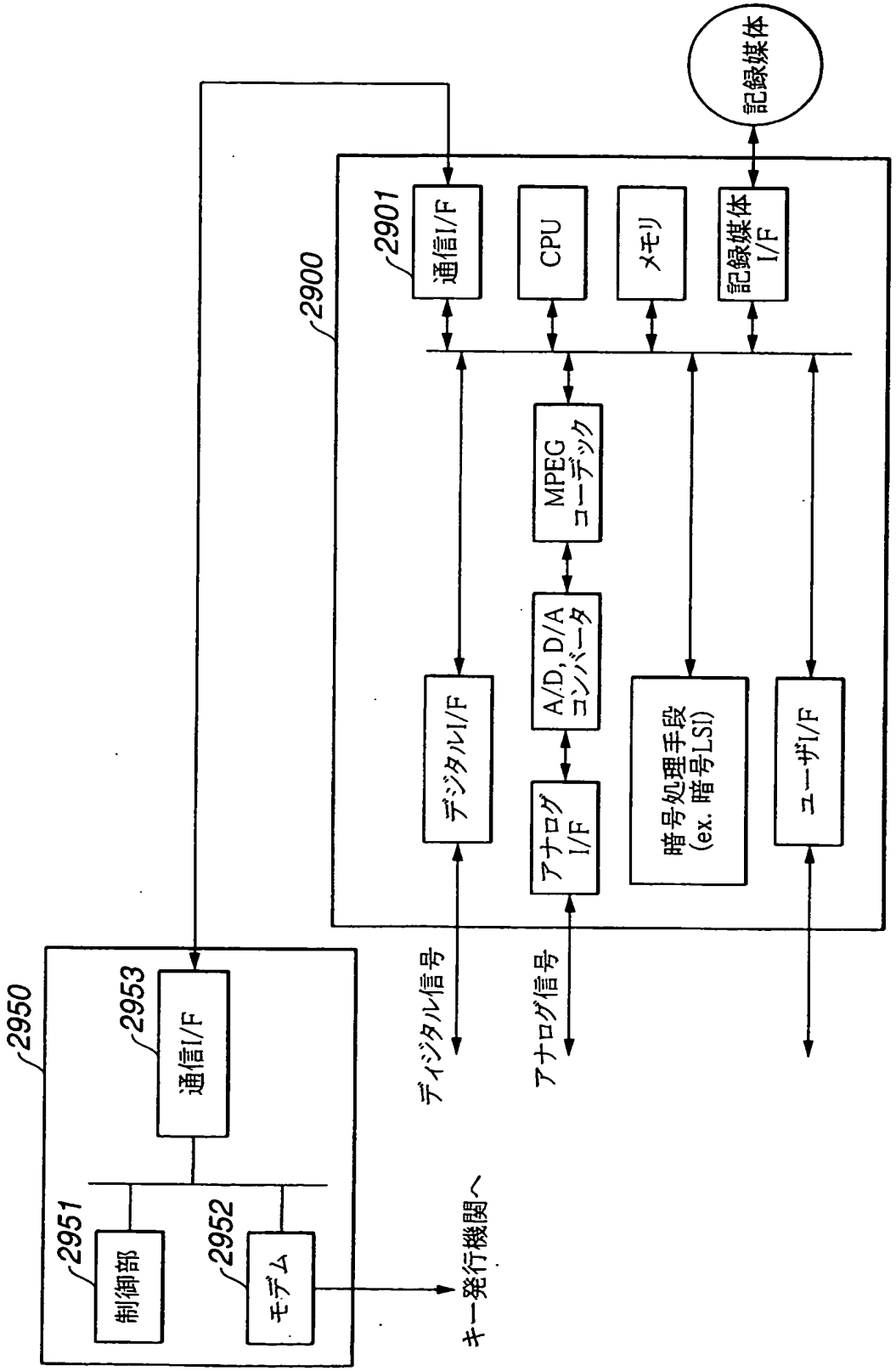

記録媒体
2900
2901
通信I/F
CPU
メモリ
記録媒体I/F
MPEGコーデック
A/D, D/Aコンバータ
デジタルI/F
アナログI/F
暗号処理手段(ex. 暗号LSI)
ユーザI/F
ディジタル信号
アナログ信号
2950
2953
通信I/F
2951
制御部
2952
モデム
キー発行機関へ

FIG.29

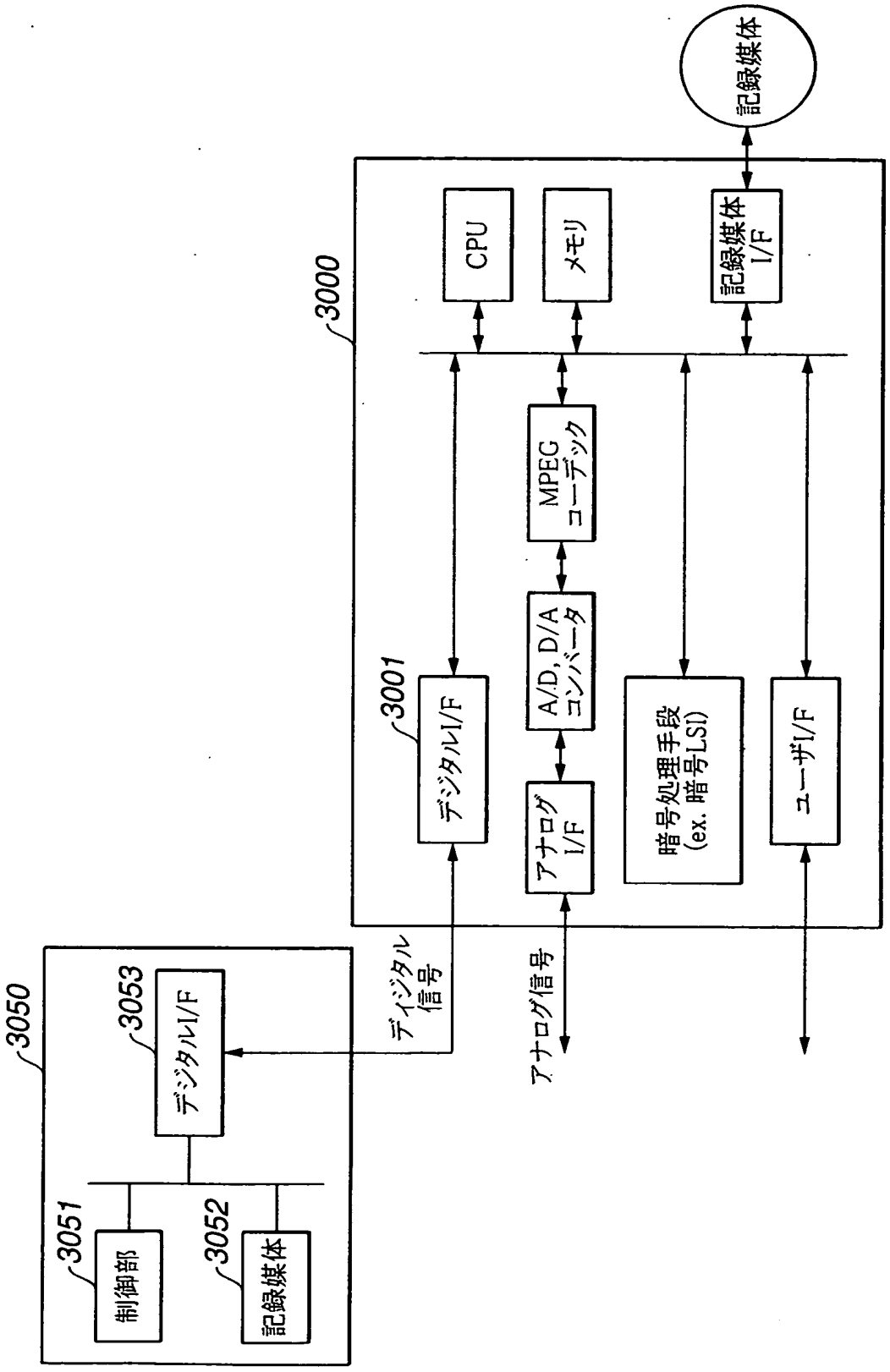

記録媒体
3000
CPU
メモリ
記録媒体 I/F
MPEG コーデック
A/D, D/A コンバータ
アナログ I/F
3001
デジタルI/F
暗号処理手段 (ex. 暗号LSI)
ユーザI/F
ディジタル信号
アナログ信号
3050
3053
デジタルI/F
3051
制御部
3052
記録媒体

FIG.30

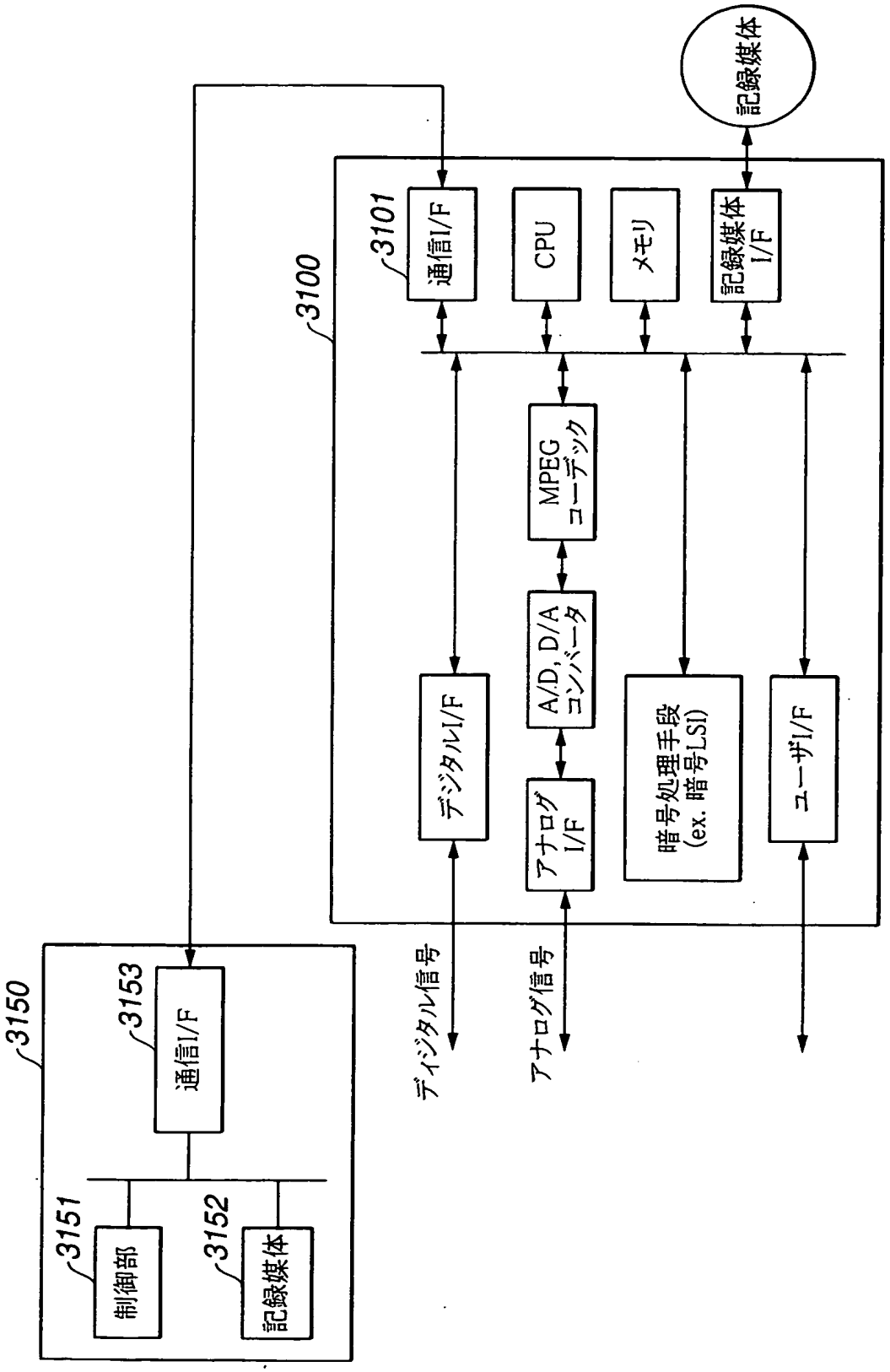

記録媒体
3100
3101
通信I/F
CPU
メモリ
記録媒体 I/F
MPEG コーデック
A/D, D/A コンバータ
デジタルI/F
アナログ I/F
暗号処理手段 (ex. 暗号LSI)
ユーザI/F
ディジタル信号
アナログ信号
3150
3153
通信I/F
3151
制御部
3152
記録媒体

FIG.31

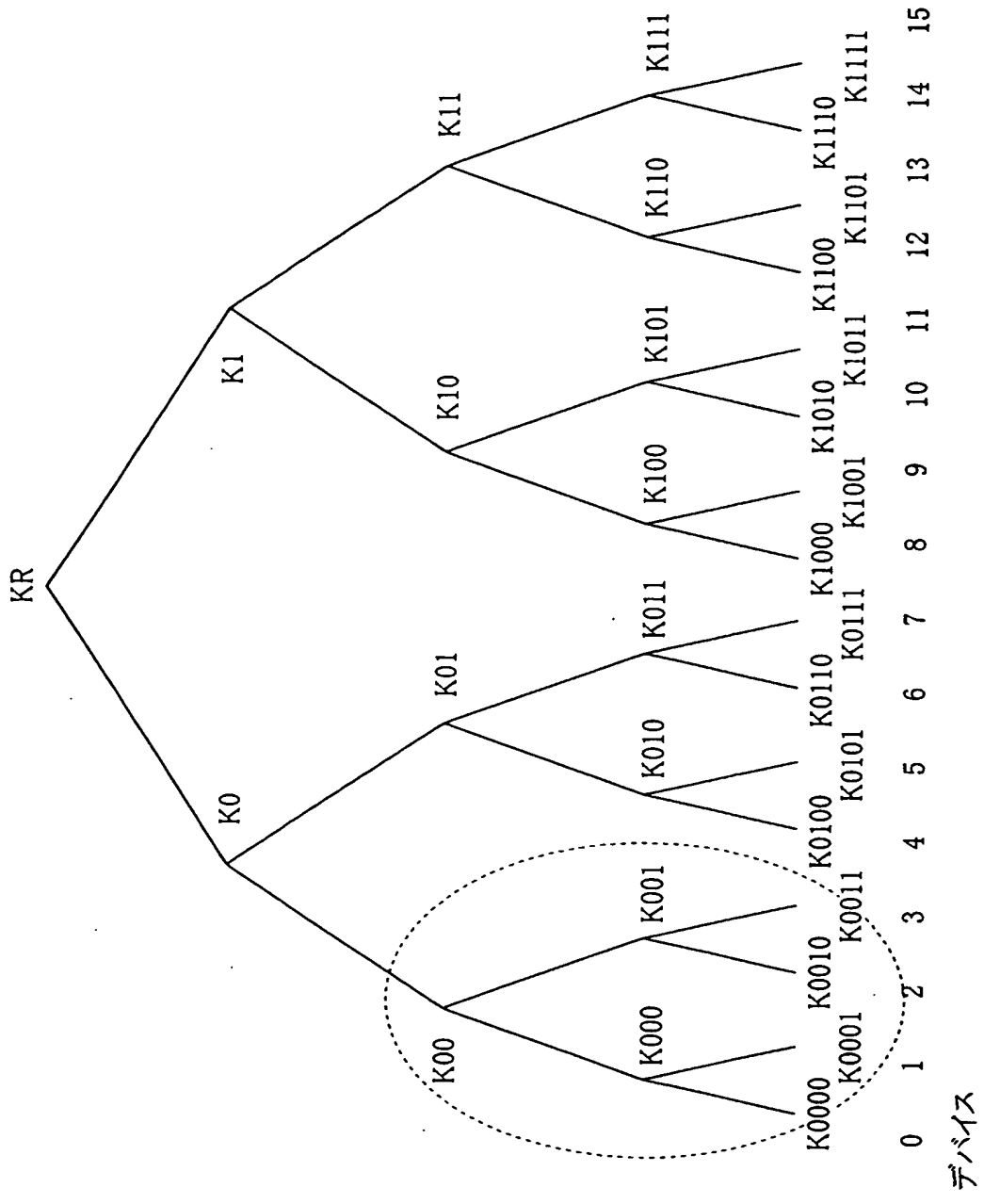

KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
デバイス

FIG.32

世代(Generation) : t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

FIG.33A

世代(Generation) : t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

FIG.33B

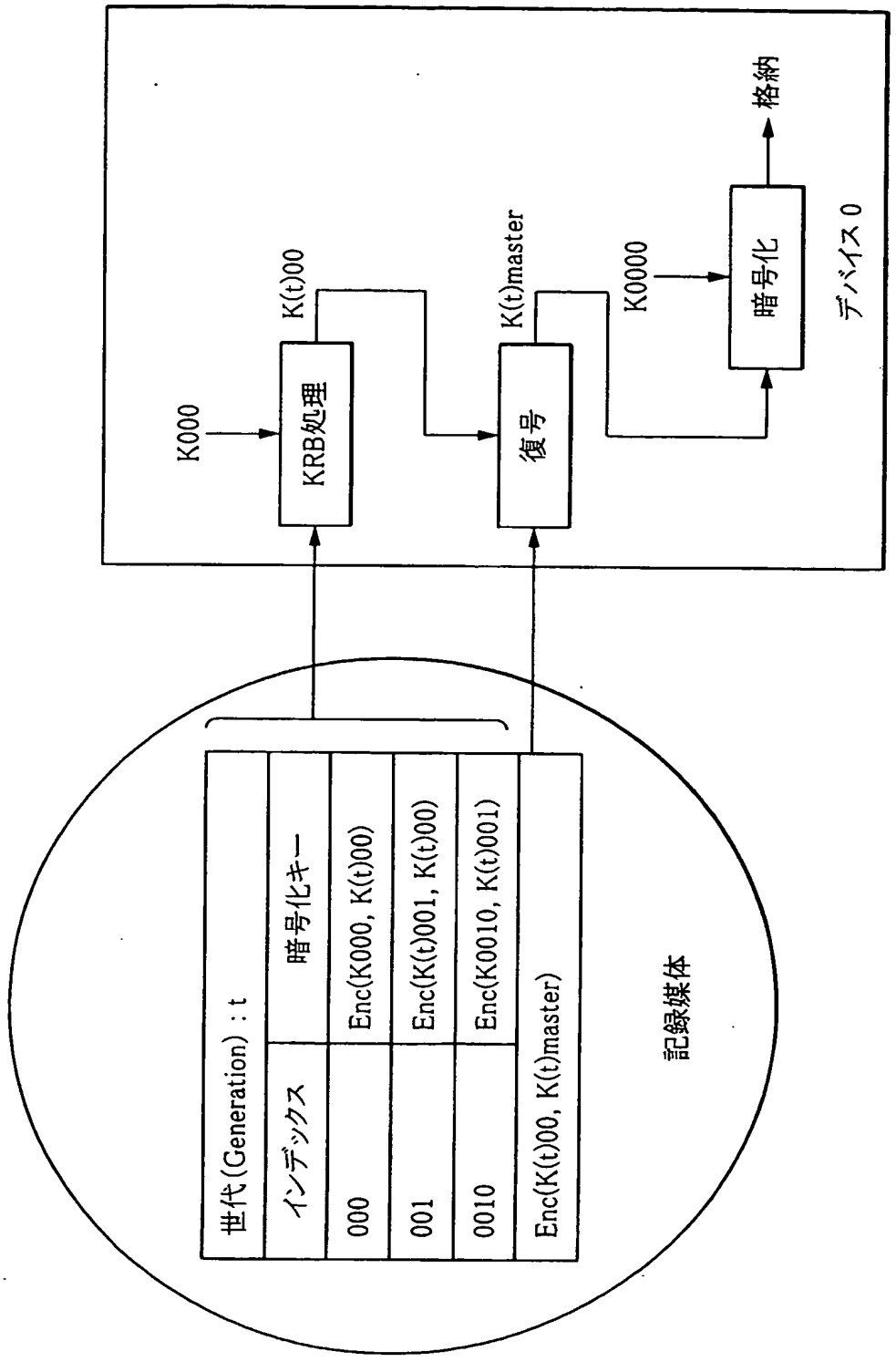

K000
KRB処理
K(t)00
復号
K(t)master
K0000
暗号化
格納
デバイス 0
記録媒体
世代(Generation) : t
インデックス
暗号化キー
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)master)

FIG.34

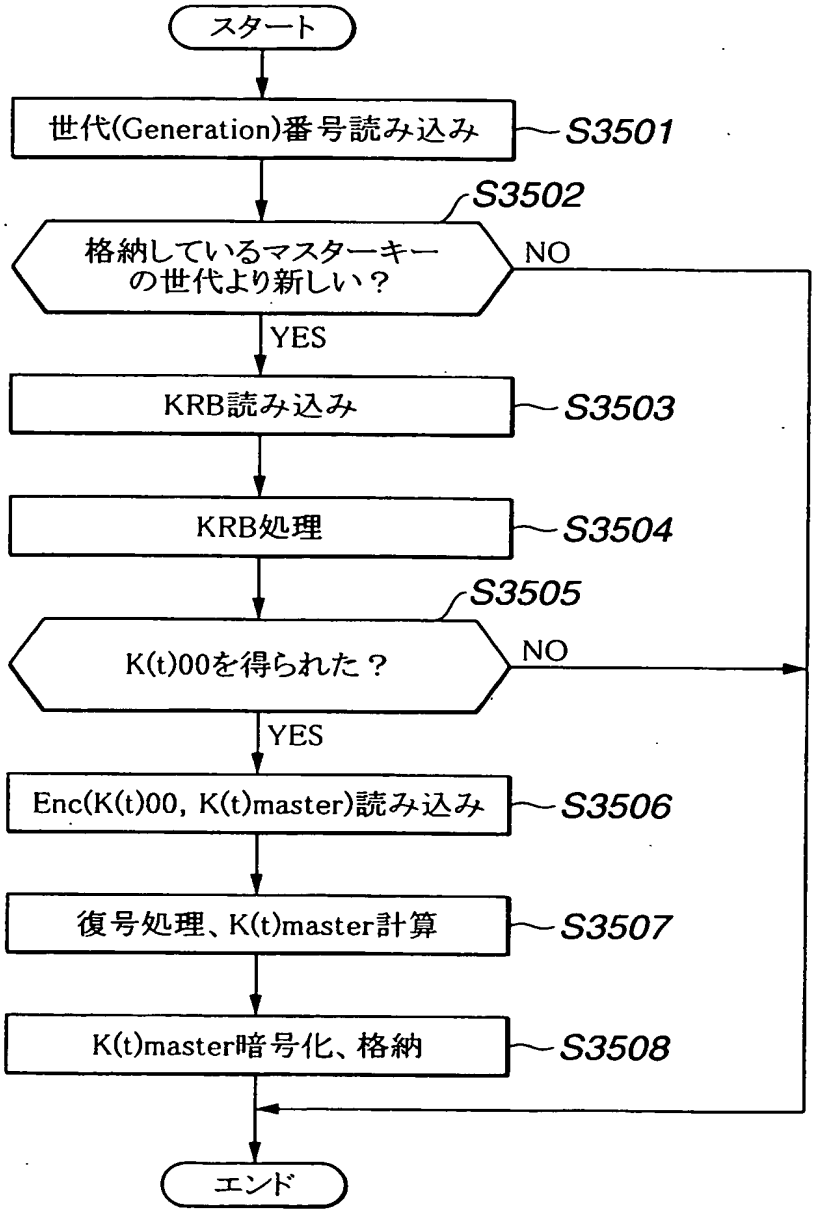

スタート
世代(Generation)番号読み込み
S3501
S3502
格納しているマスターキーの世代より新しい？
NO
YES
KRB読み込み
S3503
KRB処理
S3504
S3505
K(t)00を得られた？
NO
YES
Enc(K(t)00, K(t)master)読み込み
S3506
復号処理、K(t)master計算
S3507
K(t)master暗号化、格納
S3508
エンド

FIG.35

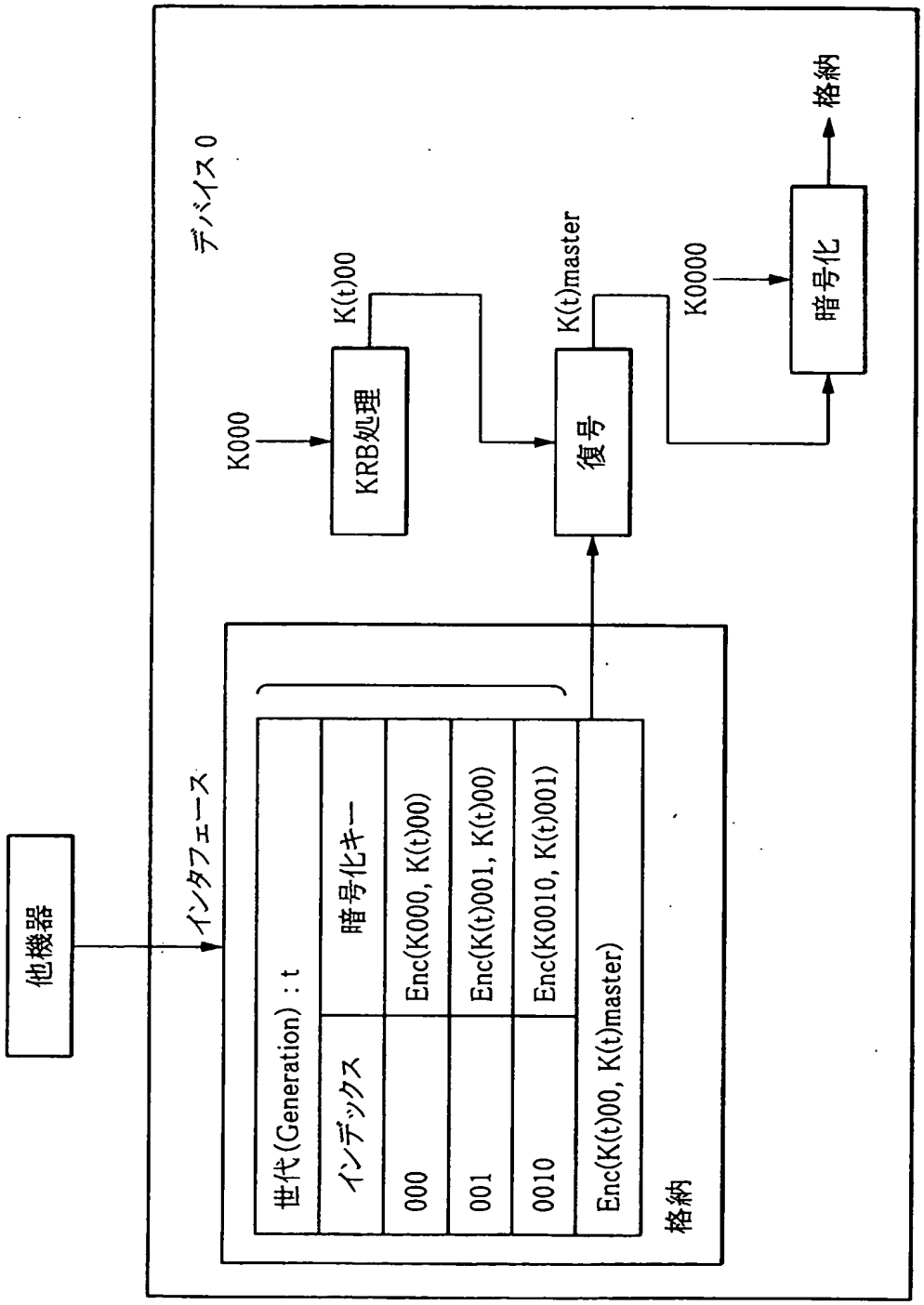

他機器
インタフェース
デバイス 0
K000
KRB処理
K(t)00
復号
K(t)master
K0000
暗号化
格納
世代(Generation) : t
インデックス
暗号化キー
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)master)
格納

FIG.36

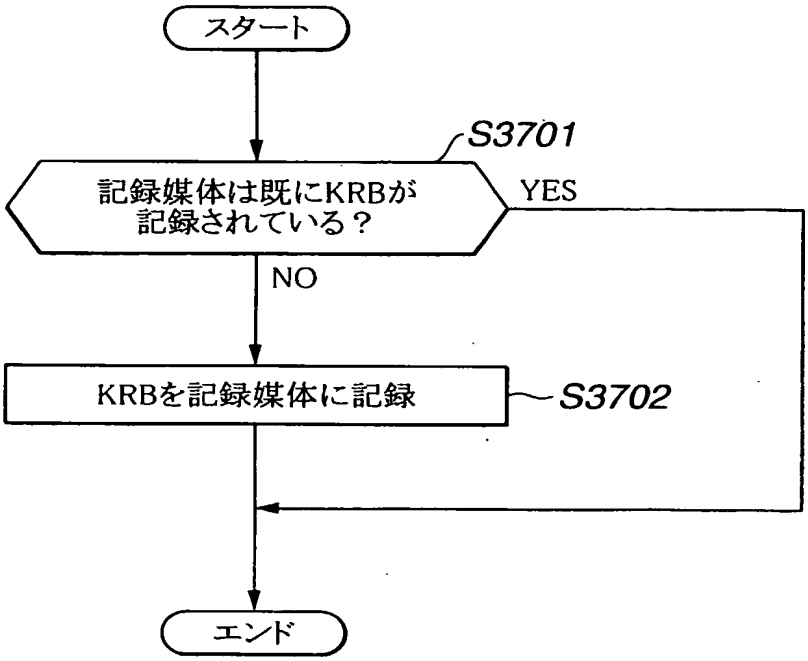

スタート
S3701
記録媒体は既にKRBが記録されている？
YES
NO
KRBを記録媒体に記録
S3702
エンド

FIG.37

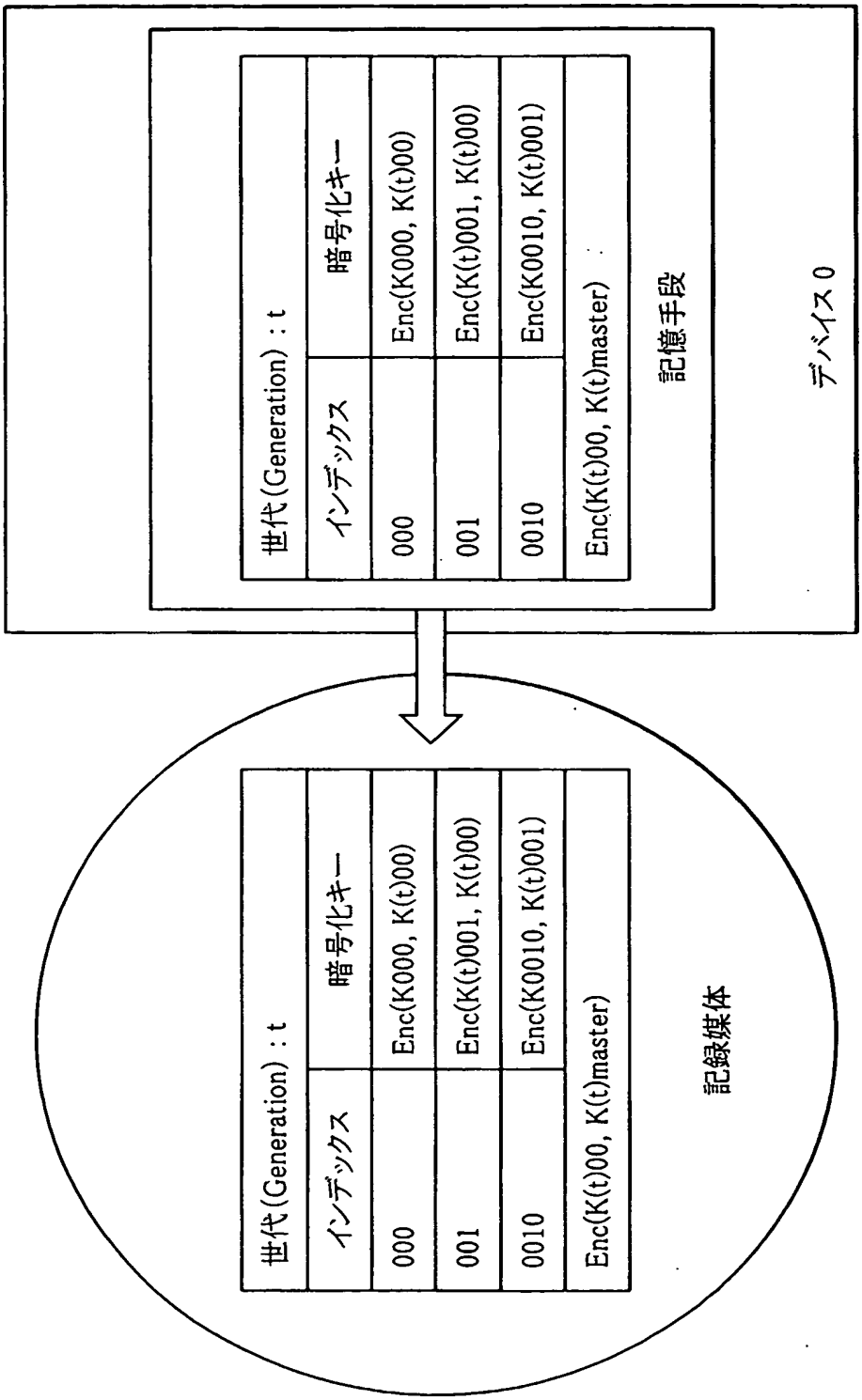

デバイス 0
記憶手段
世代(Generation) : t
インデックス
暗号化キー
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)master)
記録媒体
世代(Generation) : t
インデックス
暗号化キー
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)master)

FIG.38

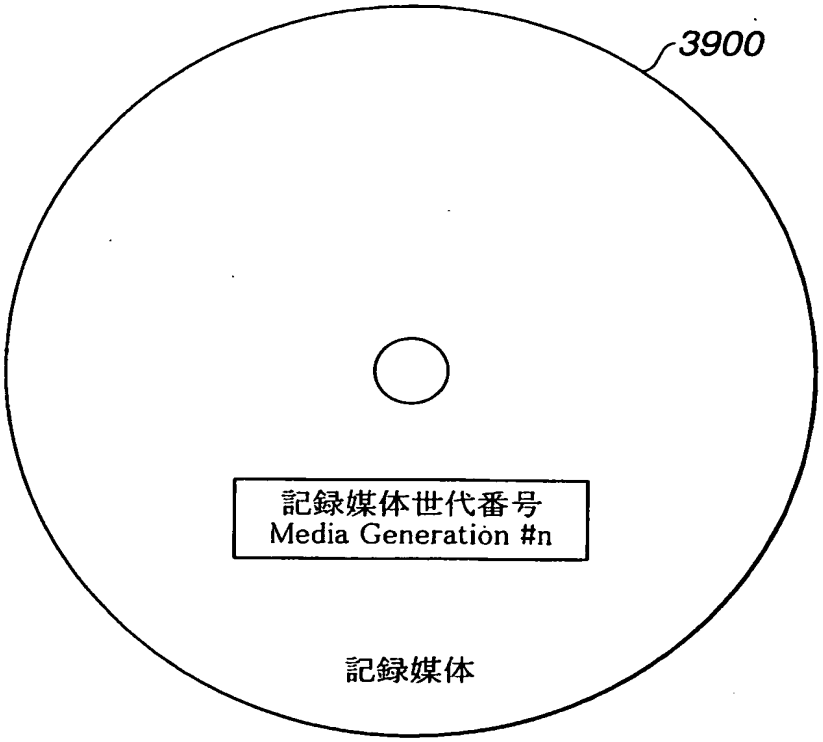


FIG.39

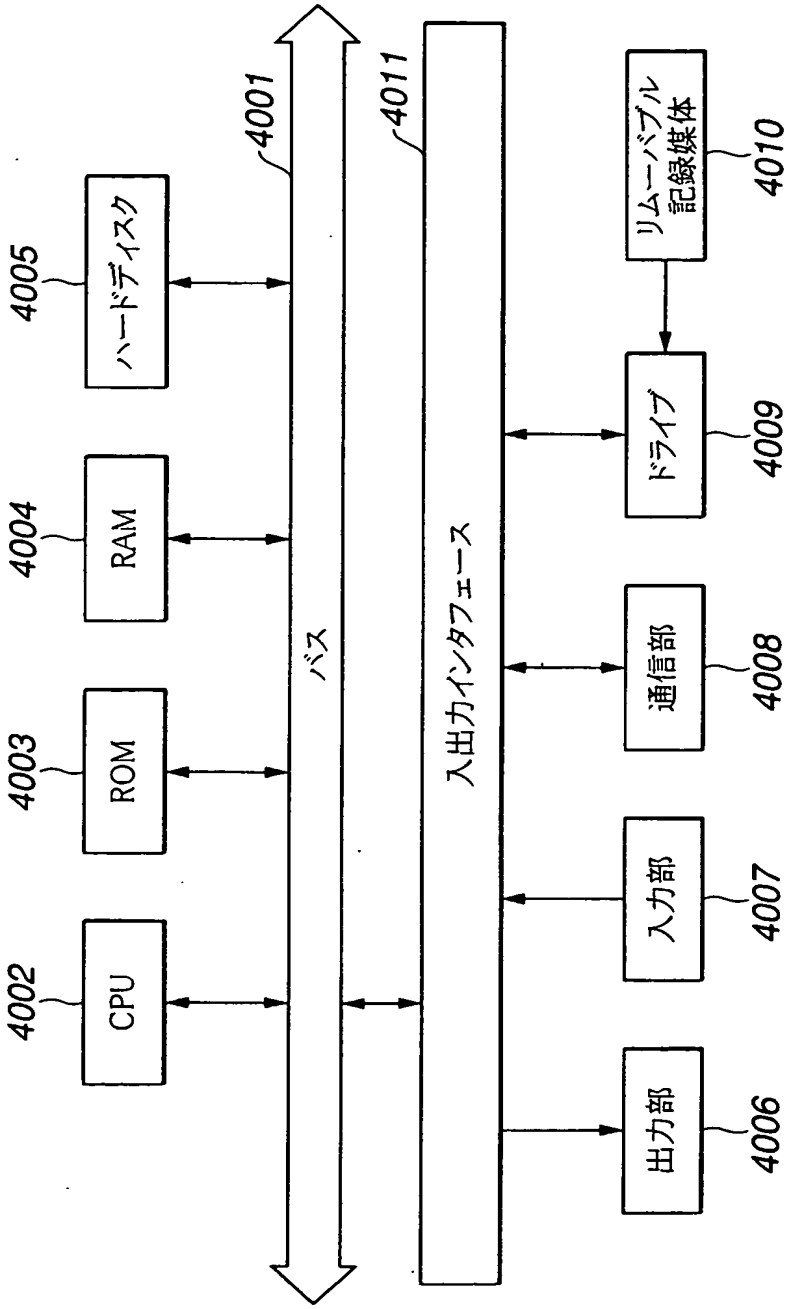

4001
4011
4005
ハードディスク
4004
RAM
4003
ROM
4002
CPU
バス
入出力インタフェース
リムーバブル記録媒体
4010
ドライブ
4009
通信部
4008
入力部
4007
出力部
4006

FIG.40

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/03004

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/00, G11B20/10, G11B20/12

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/00, G11B20/10, G11B20/12, G09C1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
WPI, JICST DATABASE ON SCIENCE AND TECHNOLOGY key, tree, generation, DVD

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP, 10-3256, A (Sony Corporation), 06 January, 1998 (06.01.98),	89,90
A	Par. Nos. [0037] to [0048] (Family: none)	1-88,91-100
A	JP, 11-39795, A (Toshiba Corporation), 12 February, 1999 (12.02.99), Full text & KR, 99013756, A & CN, 1208925, A	1-100
A	JP, 10-293726, A (Toshiba Corporation), 04 November, 1998 (04.11.98), Full text (Family: none)	1-100
A	JP, 11-250571, A (Matsushita Electric Ind. Co., Ltd.), 17 September, 1999 (17.09.99), Full text (Family: none)	1-100
A	JP, 11-250570, A (Matsushita Electric Ind. Co., Ltd.), 17 September, 1999 (17.09.99), column 13, line 17 to column 16, line 32 (Family: none)	1-100
A	JP, 11-126425, A (Sony Corporation),	1-100

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
06 July, 2001 (06.07.01)

Date of mailing of the international search report
17 July, 2001 (17.07.01)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/03004

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of the claims of the present international application are divided into the following six groups.

1. The inventions of claims 1-13, 38-51, 77, 83
2. The inventions of claims 14-30, 52-69, 78-82, 84-88
3. The inventions of claims 31-37, 70-76
4. The inventions of claims 89, 90
5. The inventions of claims 91-96
6. The inventions of claims 97-100

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

国際調査報告

国際出願番号 PCT／JP01／03004

C（続き）. 関連すると認められる文献

引用文献のカテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP 11-250571 A (松下電器産業株式会社) 17.9月.1999(17.09.99), 全頁を参照 (ファミリーなし)	1-100
A	JP 11-250570 A (松下電器産業株式会社) 17.9月.1999(17.09.99), 第13欄第17行-第16欄第32行 (ファミリーなし)	1-100
A	JP 11-126425 A (ソニー株式会社) 11.5月.1999(11.05.99), 全頁を参照 (ファミリーなし)	1-100
A	JP 11-187013 A (日本アイ・ビー・エム株式会社) 9. 7月.1999(09.07.99) 第9-11, 17-22段落 & CN 1224962 A	9-13, 26-30, 33-37, 65-69, 72-76, 79-88, 98, 100
A	WALDVOGEL, M. et al. The VersaKey Framework:Versatile Group Key Management. IEEE Journal on Selected Areas in Communications. Septemper 1999, Vol.17, No.9 , p.1614-1631, especially pp.1616-1621	9-13, 26-30, 33-37, 65-69, 72-76, 79-88, 98, 100
A	WONG, C.K. et al. Secure Group Communications Using Key Graphs. In: Proceedings of ACM SIGCOMM'98 , 1998 , p.68-79 especially 3.4 Leaving a tree key graph (http://www.acm.org/sigcomm/sigcomm98/tp/technical.html)	9-13, 26-30, 33-37, 65-69, 72-76, 79-88, 98, 100
A	5C Digital Transmission Content Protection White Paper. Revision 1.0, 1998, p.3, 11, 12 (http://www.dtcp.com)	1-100
PA	館林誠 他, 記録メディアのコンテンツ保護システム, 2000年電子情報通信学会基礎・境界ソサイエティ大会講演論文集, 7.9月.2000(07.09.00), p.367-368	1-100

国際調査報告

国際出願番号 PCT／JP01／03004

A. 発明の属する分野の分類（国際特許分類（IPC））

Int. Cl' H04L9／00, G11B20／10, G11B20／12

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl' H04L9／00, G11B20／10, G11B20／12, G09C1／00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2001年
日本国登録実用新案公報	1994－2001年
日本国実用新案登録公報	1996－2001年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

WPI, JICST科学技術文献データベース key, tree, generation, DVD

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP 10-3256 A (ソニー株式会社) 6.1月.1998(06.01.98), 第37-48段落 (ファミリーなし)	89, 90
A		1-88, 91-100
A	JP 11-39795 A (株式会社東芝) 12.2月.1999(12.02.99), 全頁を参照 & KR 99013756 A & CN 1208925 A	1-100
A	JP 10-293726 A (株式会社東芝) 4.11月.1998(04.11.98), 全頁を参照 (ファミリーなし)	1-100

☒ C欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日 06. 07. 01	国際調査報告の発送日 17.07.01
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 中里 裕正 5M 9364 電話番号 03－3581－1101 内線 3597

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０１／０３００４

第Ⅰ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、

2. ☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3. ☐ 請求の範囲 _____ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅱ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

この出願の発明は、下記の６群の発明に区分される。

1. 請求の範囲 1-13, 38-51, 77, 83
2. 請求の範囲14-30, 52-69, 78-82, 84-88
3. 請求の範囲31-37, 70-76
4. 請求の範囲89, 90
5. 請求の範囲91-96
6. 請求の範囲97-100

1. ☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

特許協力条約に基づく国際出願願書
副本 - 印刷日時 2001年04月06日 (06.04.2001) 金曜日 15時21分10秒

SK01PCT44

PCT
06.4.01
受領印

0	受理官庁記入欄	
0-1	国際出願番号.	
0-2	国際出願日	
0-3	(受付印)	
0-4	様式-PCT/RO/101 この特許協力条約に基づく国際出願願書は、	
0-4-1	右記によって作成された。	PCT-EASY Version 2.91 (updated 01.01.2001)
0-5	申立て 出願人は、この国際出願が特許協力条約に従って処理されることを請求する。	
0-6	出願人によって指定された受理官庁	日本国特許庁 (RO/JP)
0-7	出願人又は代理人の書類記号	SK01PCT44
I	発明の名称	情報記録装置、情報再生装置、情報記録方法、情報再生方法
II	出願人	
II-1	この欄に記載した者は	出願人である (applicant only)
II-2	右の指定国についての出願人である。	米国を除くすべての指定国 (all designated States except US)
II-4ja	名称	ソニー株式会社
II-4en	Name	SONY CORPORATION
II-5ja	あて名:	141-0001 日本国 東京都 品川区 北品川６丁目７番３５号
II-5en	Address:	7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
II-6	国籍 (国名)	日本国 JP
II-7	住所 (国名)	日本国 JP
III-1	その他の出願人又は発明者	
III-1-1	この欄に記載した者は	出願人及び発明者である (applicant and inventor)
III-1-2	右の指定国についての出願人である。	米国のみ (US only)
III-1-4ja	氏名(姓名)	浅野 智之
III-1-4en	Name (LAST, First)	ASANO, Tomoyuki
III-1-5ja	あて名:	141-0001 日本国 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内
III-1-5en	Address:	c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
III-1-6	国籍 (国名)	日本国 JP
III-1-7	住所 (国名)	日本国 JP

III-2	その他の出願人又は発明者	
III-2-1	この欄に記載した者は	出願人及び発明者である (applicant and inventor)
III-2-2	右の指定国についての出願人である。	米国のみ (US only)
III-2-4ja	氏名(姓名)	大澤 義知
III-2-4en	Name (LAST, First)	OSAWA, Yoshitomo
III-2-5ja	あて名:	141-0001 日本国 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内
III-2-5en	Address:	c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
III-2-6	国籍 (国名)	日本国 JP
III-2-7	住所 (国名)	日本国 JP
III-3	その他の出願人又は発明者	
III-3-1	この欄に記載した者は	出願人及び発明者である (applicant and inventor)
III-3-2	右の指定国についての出願人である。	米国のみ (US only)
III-3-4ja	氏名(姓名)	石黒 隆二
III-3-4en	Name (LAST, First)	ISHIGURO, Ryuji
III-3-5ja	あて名:	141-0001 日本国 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内
III-3-5en	Address:	c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
III-3-6	国籍 (国名)	日本国 JP
III-3-7	住所 (国名)	日本国 JP
III-4	その他の出願人又は発明者	
III-4-1	この欄に記載した者は	出願人及び発明者である (applicant and inventor)
III-4-2	右の指定国についての出願人である。	米国のみ (US only)
III-4-4ja	氏名(姓名)	光澤 敦
III-4-4en	Name (LAST, First)	MITSUZAWA, Atsushi
III-4-5ja	あて名:	141-0001 日本国 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内
III-4-5en	Address:	c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
III-4-6	国籍 (国名)	日本国 JP
III-4-7	住所 (国名)	日本国 JP

特許協力条約に基づく国際出願願書 SK01PCT44
副本 - 印刷日時 2001年04月06日 (06.04.2001) 金曜日 15時21分10秒

III-5	その他の出願人又は発明者	
III-5-1	この欄に記載した者は	出願人及び発明者である (applicant and inventor)
III-5-2	右の指定国についての出願人である。	米国のみ (US only)
III-5-4ja	氏名(姓名)	大石 丈於
III-5-4en	Name (LAST, First)	OISHI, Tateo
III-5-5ja	あて名:	141-0001 日本国 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内
III-5-5en	Address:	c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
III-5-6	国籍 (国名)	日本国 JP
III-5-7	住所 (国名)	日本国 JP
III-6	その他の出願人又は発明者	
III-6-1	この欄に記載した者は	出願人及び発明者である (applicant and inventor)
III-6-2	右の指定国についての出願人である。	米国のみ (US only)
III-6-4ja	氏名(姓名)	瀧 隆太
III-6-4en	Name (LAST, First)	TAKI, Ryuta
III-6-5ja	あて名:	141-0001 日本国 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内
III-6-5en	Address:	c/o SONY CORPORATION 7-35, Kitashinagawa 6-chome Shinagawa-ku, Tokyo 141-0001 Japan
III-6-6	国籍 (国名)	日本国 JP
III-6-7	住所 (国名)	日本国 JP
IV-1	代理人又は共通の代表者、通知のあて名 下記の者は国際機関において右記のごとく出願人のために行動する。	代理人 (agent)
IV-1-1ja	氏名(姓名)	小池 晃
IV-1-1en	Name (LAST, First)	KOIKE, Akira
IV-1-2ja	あて名:	105-0001 日本国 東京都 港区 虎ノ門二丁目６番４号 第１１森ビル
IV-1-2en	Address:	No.11 Mori Bldg., 6-4, Toranomon 2-chome Minato-ku, Tokyo 105-0001 Japan
IV-1-3	電話番号	03-3508-8266
IV-1-4	ファクシミリ番号	03-3508-0439

特許協力条約に基づく国際出願願書 SK01PCT44
副本 - 印刷日時 2001年04月06日 (06.04.2001) 金曜日 15時21分10秒

IV-2	その他の代理人	筆頭代理人と同じあて名を有する代理人 (additional agent(s) with same address as first named agent)
IV-2-1ja	氏名	田村 榮一; 伊賀 誠司
IV-2-1en	Name(s)	TAMURA, Eiichi; IGA, Seiji
V	国の指定	
V-1	広域特許 (他の種類の保護又は取扱いを求める場合には括弧内に記載する。)	AP: GH GM KE LS MW MZ SD SL SZ TZ UG ZW 及びハラレプロトコルと特許協力条約の締約国である他の国 EA: AM AZ BY KG KZ MD RU TJ TM 及びユーラシア特許条約と特許協力条約の締約国である他の国 EP: AT BE CH&LI CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR 及びヨーロッパ特許条約と特許協力条約の締約国である他の国 OA: BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG 及びアフリカ知的所有権機構と特許協力条約の締約国である他の国
V-2	国内特許 (他の種類の保護又は取扱いを求める場合には括弧内に記載する。)	AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH&LI CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
V-5	指定の確認の宣言 出願人は、上記の指定に加えて、規則4.9(b)の規定に基づき、特許協力条約のもとで認められる他の全ての国の指定を行う。ただし、V-6欄に示した国の指定を除く。出願人は、これらの追加される指定が確認を条件としていること、並びに優先日から15月が経過する前にその確認がなされない指定は、この期間の経過時に、出願人によって取り下げられたものとみなされることを宣言する。	
V-6	指定の確認から除かれる国	なし (NONE)
VI-1	先の国内出願に基づく優先権主張	
VI-1-1	先の出願日	2000年04月06日 (06.04.2000)
VI-1-2	先の出願番号	特願2000-105328
VI-1-3	国名	日本国 JP
VI-2	先の国内出願に基づく優先権主張	
VI-2-1	先の出願日	2000年04月07日 (07.04.2000)
VI-2-2	先の出願番号	特願2000-106039
VI-2-3	国名	日本国 JP

特許協力条約に基づく国際出願願書 SK01PCT44

副本 - 印刷日時 2001年04月06日 (06.04.2001) 金曜日 15時21分10秒

VI-3	先の国内出願に基づく優先権主張		
VI-3-1	先の出願日	2000年06月07日 (07.06.2000)	
VI-3-2	先の出願番号	特願2000-170604	
VI-3-3	国名	日本国 JP	
VI-4	先の国内出願に基づく優先権主張		
VI-4-1	先の出願日	2000年12月25日 (25.12.2000)	
VI-4-2	先の出願番号	特願2000-391976	
VI-4-3	国名	日本国 JP	
VII-1	特定された国際調査機関(ISA)	日本国特許庁 (ISA/JP)	
VIII	照合欄	用紙の枚数	添付された電子データ
VIII-1	願書	6	-
VIII-2	明細書	70	-
VIII-3	請求の範囲	23	-
VIII-4	要約	1	absk01pct44.txt
VIII-5	図面	37	-
VIII-7	合計	137	
	添付書類	添付	添付された電子データ
VIII-8	手数料計算用紙	✓	-
VIII-9	別個の記名押印された委任状	✓	-
VIII-10	包括委任状の写し	✓	-
VIII-12	優先権証明書	優先権証明書 VI-1, VI-2, VI-3, VI-4	-
VIII-16	PCT-EASYディスク	-	フレキシブルディスク
VIII-17	その他	納付する手数料に相当する特許印紙を貼付した書面	-
VIII-17	その他	国際事務局の口座への振込を証明する書面	-
VIII-18	要約書とともに提示する図の番号	14	
VIII-19	国際出願の使用言語名:	日本語 (Japanese)	
IX-1	提出者の記名押印		
IX-1-1	氏名(姓名)	小池 晃	
IX-2	提出者の記名押印		
IX-2-1	氏名(姓名)	田村 榮一	
IX-3	提出者の記名押印		
IX-3-1	氏名(姓名)	伊賀 誠司	

受理官庁記入欄

10-1	国際出願として提出された書類の実際の受理の日	
10-2	図面 :	
10-2-1	受理された	
10-2-2	不足図面がある	

特許協力条約に基づく国際出願願書 SK01PCT44

副本 - 印刷日時 2001年04月06日 (06.04.2001) 金曜日 15時21分10秒

10-3	国際出願として提出された書類を補完する書類又は図面であってその後期間内に提出されたものの実際の受理の日（訂正日）	
10-4	特許協力条約第11条(2)に基づく必要な補完の期間内の受理の日	
10-5	出願人により特定された国際調査機関	ISA/JP
10-6	調査手数料未払いにつき、国際調査機関に調査用写しを送付していない	

国際事務局記入欄

11-1	記録原本の受理の日	

EP ・ US　　PCT

特　許　協　力　条　約

国際調査報告

（法８条、法施行規則第40、41条）
〔ＰＣＴ１８条、ＰＣＴ規則43、44〕

出願人又は代理人の書類記号　ＳＫ０１ＰＣＴ４４	今後の手続きについては、国際調査報告の送付通知様式（ＰＣＴ／ＩＳＡ／２２０）及び下記５を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ０１／０３００４	国際出願日 （日.月.年）　０６．０４．０１	優先日 （日.月.年）　０６．０４．００
出願人（氏名又は名称） ソニー株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条（ＰＣＴ１８条）の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で　4　ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

１．国際調査報告の基礎

ａ．言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。
☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

ｂ．この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。
☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際調査機関に提出された書面による配列表
☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

２．☐ 請求の範囲の一部の調査ができない（第Ｉ欄参照）。

３．☒ 発明の単一性が欠如している（第Ⅱ欄参照）。

４．発明の名称は
☐ 出願人が提出したものを承認する。
☒ 次に示すように国際調査機関が作成した。
情報記録／再生装置及び方法

５．要約は
☒ 出願人が提出したものを承認する。
☐ 第Ⅲ欄に示されているように、法施行規則第47条（ＰＣＴ規則38.2(b)）の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から１カ月以内にこの国際調査機関に意見を提出することができる。

６．要約書とともに公表される図は、
第　１４　図とする。☒ 出願人が示したとおりである。　☐ なし
☐ 出願人は図を示さなかった。
☐ 本図は発明の特徴を一層よく表している。

国際調査[redacted]　　国際出願番号[redacted]CT／JP01／03004

第Ⅰ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第８条第３項（ＰＣＴ１７条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1．☐ 請求の範囲 _____は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

2．☐ 請求の範囲 _____は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

3．☐ 請求の範囲 _____は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第３文の規定に従って記載されていない。

第Ⅱ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

この出願の発明は、下記の６群の発明に区分される。

1．請求の範囲 1-13, 38-51, 77, 83
2．請求の範囲14-30, 52-69, 78-82, 84-88
3．請求の範囲31-37, 70-76
4．請求の範囲89, 90
5．請求の範囲91-96
6．請求の範囲97-100

1．☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。

2．☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。

3．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。

4．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。

☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。

国際調査報[redacted]　　国際出願番号[redacted]CT／JP01／03004

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷　H04L9／00, G11B20／10, G11B20／12

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷　H04L9／00, G11B20／10, G11B20／12, G09C1／00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2001年
日本国登録実用新案公報	1994－2001年
日本国実用新案登録公報	1996－2001年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

WPI, JICST科学技術文献データベース　key, tree, generation, DVD

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP 10-3256 A (ソニー株式会社) 6.1月.1998(06.01.98), 第37-48段落 (ファミリーなし)	89,90
A		1-88,91-100
A	JP 11-39795 A (株式会社東芝) 12.2月.1999(12.02.99), 全頁を参照 & KR 99013756 A & CN 1208925 A	1-100
A	JP 10-293726 A (株式会社東芝) 4.11月.1998(04.11.98), 全頁を参照 (ファミリーなし)	1-100

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日　06.07.01	国際調査報告の発送日　17.07.01
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 中里　裕正　　5M　9364 電話番号　03－3581－1101　内線　3597

様式PCT／ISA／210（第2ページ）（1998年7月）

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP 11-250571 A (松下電器産業株式会社) 17.9月.1999(17.09.99), 全頁を参照 (ファミリーなし)	1-100
A	JP 11-250570 A (松下電器産業株式会社) 17.9月.1999(17.09.99), 第13欄第17行-第16欄第32行 (ファミリーなし)	1-100
A	JP 11-126425 A (ソニー株式会社) 11.5月.1999(11.05.99), 全頁を参照 (ファミリーなし)	1-100
A	JP 11-187013 A (日本アイ・ビー・エム株式会社) 9. 7月.1999(09.07.99) 第9-11, 17-22段落 & CN 1224962 A	9-13, 26-30, 33-37, 65-69, 72-76, 79-88, 98, 100
A	WALDVOGEL, M. et al. The VersaKey Framework:Versatile Group Key Management. IEEE Journal on Selected Areas in Communications. Septemper 1999, Vol.17, No.9 , p.1614-1631, especially pp.1616-1621	9-13, 26-30, 33-37, 65-69, 72-76, 79-88, 98, 100
A	WONG, C.K. et al. Secure Group Communications Using Key Graphs. In: Proceedings of ACM SIGCOMM'98 , 1998 , p.68-79 especially 3.4 Leaving a tree key graph (http://www.acm.org/sigcomm/sigcomm98/tp/technical.html)	9-13, 26-30, 33-37, 65-69, 72-76, 79-88, 98, 100
A	5C Digital Transmission Content Protection White Paper. Revision 1.0, 1998, p.3, 11, 12 (http://www.dtcp.com)	1-100
PA	館林誠 他, 記録メディアのコンテンツ保護システム, 2000年電子情報通信学会基礎・境界ソサイエティ大会講演論文集, 7.9月.2000(07.09.00), p.367-368	1-100